IBM Intelligent Operations Center

IBM Intelligent Operations Center Documentación del producto

Versión 1 Release 5

IBM Intelligent Operations Center

IBM Intelligent Operations Center Documentación del producto

Versión 1 Release 5

Nota
Antes de utilizar esta información y el producto al que da soporte, lea la información de "Avisos" en la página 369.

Esta edición se aplica a IBM Intelligent Operations Center versión 1, release 5, modificación 0. Esta edición se aplica a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Contenido

Figuras

Capítulo 1. Visión general de la solución

Muchas organizaciones y esfuerzos requieren una coordinación y supervisión operativa eficiente. Todos tienen en común, la necesidad de reunir una información correcta para que las personas adecuadas puedan tomar decisiones rápidas y acertadas y hacer un seguimiento del efecto de esas decisiones. El IBM® Intelligent Operations Center es una solución de software diseñada para facilitar la coordinación y supervisión eficaz de las operaciones.

Las autoridades se enfrentan a retos comunes en sus sistemas núcleo y a la hora de hacer mejoras a sistemas que están interconectados. Las autoridades de amplias miras quieren utilizar las mejoras en rendimiento y eficacia de los sistemas núcleo más inteligentes. Adoptan nuevas formas de pensar y el uso de estos sistemas. La aplicación de tecnología de la información avanzada puede ayudar a las autoridades a entender mejor, predecir y responder inteligentemente a patrones de comportamiento y sucesos.

Por ejemplo, IBM define una ciudad inteligente en términos de mejora en calidad de vida y bienestar económico que se logran aplicando las tecnología de la información (IT) para planificar, diseñar, compilar y operar la infraestructura de la ciudad. Una ciudad inteligente no tiene que ver principalmente con "la tecnología más reciente." Tiene que ver con encontrar formas de utilizar la tecnología para hacer un uso más eficiente de los recursos existentes, para mejorar la vida de los ciudadanos de la ciudad.

El IBM Intelligent Operations Center utiliza el poder de los datos de la vida real generados por sistemas informáticos para la:

- Recopilación y gestión de los datos correctos
- Integración y el análisis de esos datos
- Facilitar un acceso rápido y puntual a la información
- Presentar información relacionada de una manera coherente

Los beneficios de esta solución son:

- Ajustar los sistemas para lograr resultados basándose en los conocimientos adquiridos
- Optimizar las operaciones planificadas y no planificadas utilizando una creación de informes holística y supervisando el enfoque
- Crear convergencia de dominios en una organización facilitando la comunicación y la colaboración
- Mejorar la calidad del servicio y reducir los gastos coordinando sucesos

Una operación se puede dividir en dominios individuales, que generalmente coinciden con la estructura de la organización y la experiencia de las personas implicadas. En una ciudad, la experiencia la tienen los departamentos, por ejemplo en transporte, agua y seguridad pública.

A medida que la complejidad de las operaciones en un dominio aumenta, se requiere una solución más personalizada. El IBM Intelligent Operations Center tiene muchos puntos de integración diferentes donde puede tener lugar la personalización. Estos puntos de integración y la infraestructura incluida proporcionan a IBM Business Partners, los proveedores de servicio y a los clientes la flexibilidad para crear un solución amplia y de gran alcance.

Destinatarios

Este Information Center va dirigido a las personas que utilizan, instalan, administran y mantienen IBM Intelligent Operations Center. También contiene documentación de implementación para personalizar la solución e integrar los sistemas subyacentes externos que requiere IBM Intelligent Operations Center .

Este centro de información se basa en la suposición de que los usuarios tienen conocimientos previos o dominio del uso de los productos componentes incluidos en esta solución. El centro de información también da por supuesto que los usuarios tienen conocimientos básicos del sistema operativo Red Hat Enterprise Linux. Este centro de información no incluye la formación para utilizar los productos componentes o el sistema operativo. Si requiere formación sobre estos productos, consulte con su integrador de sistemas o con el representante de IBM para obtener información sobre oportunidades de formación de componentes básicos.

Puede encontrar enlaces a la documentación del producto del componente en sección Referencia, para ello siga el enlace que encontrará al final de este tema.

Conceptos relacionados:

"Información adicional sobre el producto" en la página 366
Los siguientes recursos adicionales están disponibles en línea.

Características

El IBM Intelligent Operations Center proporciona prestaciones de medición, supervisión y modelado que integran sistemas subyacentes en una solución para mejorar la eficiencia operativa, la planificación y la coordinación.

El IBM Intelligent Operations Center es una solución dentro de la familia de productos IBM Smarter Cities Software Solutions . IBM Intelligent Operations Center se puede instalar en el hardware existente (en principio) o se puede desplegar en la nube. IBM Intelligent Operations Center se puede instalar solo o con otras soluciones de la familia de productos de IBM Smarter Cities Software Solutions.

El IBM Intelligent Operations Center es una solución basada en la GUI con acceso basado en roles a los sucesos para una organización y dominios subyacentes. Tiene gestión de sucesos, correlación integrada y capacidades de supervisión de recursos. La solución puede proporcionar y realizar un seguimiento de los procedimientos y del flujo de trabajo adecuados para las actividades como preparación y respuesta a los sucesos. También tiene indicador de rendimiento clave (KPI) y funciones de colaboración para una efectividad mejorada. Estas funciones proporcionan autoridades con la capacidad de integrar dominios para una mejor cooperación y toma de decisiones.

Gestión de sucesos e incidencias

IBM Intelligent Operations Center proporciona un mecanismo de generación de informes sobre sucesos y de rastreo para permitir la identificación y la comprensión en dominios subyacentes. Puede gestionar sucesos previstos, sucesos planeados o sucesos actuales a medida que se desarrollan. Por ejemplo, sustituir unas tuberías situadas debajo de la calzadas son un suceso planificado o un pedido de trabajo que implica operaciones de agua y de tráfico. Las inclemencias del clima pronosticadas para las próximas 24 horas son un suceso previsto. Un atasco de tráfico es un suceso actual afectado por las obras en la carretera y por el clima.

Un sistema de información geográfica (GIS) integrado o un plan de ubicación correlaciona sucesos de forma visual, para que pueda medir su impacto a través de la correlación interactiva y el análisis de escenarios.

Gestión de recursos, respuestas y actividades

IBM Intelligent Operations Center proporciona un sistema para almacenar procedimientos y flujos de trabajo adecuados basándose en actividades asociadas con sucesos. Puede realizar un seguimiento del progreso de los flujos de trabajo y supervisar o actualizar el estado de las actividades que se le asignen.

Puede resaltar información sobre una serie de recursos disponibles en un mapa. La información es de fácil acceso cuando y donde lo desee.

Supervisión de estado

IBM Intelligent Operations Center proporciona una herramienta para crear y mostrar KPI. Los KPI se pueden actualizar como cambios de datos subyacentes. Puede utilizar esta herramienta para:

- Resumir el estado a nivel ejecutivo para un único dominio o en dominios
- Destacar los problemas e identificarlos
- Investigar más profundizando en los detalles de KPI

Notificación instantánea y mensajería

IBM Intelligent Operations Center proporciona un espacio de trabajo donde puede mantener alertas para cuestiones que necesitan atención. Puede utilizar este espacio de trabajo para supervisar noticias y sucesos, especialmente cuando otros portlets que anuncian noticias no están a la vista.

IBM Lotus Sametime proporciona una colaboración integrada y una herramienta de comunicación que puede utilizar para los mensajes instantáneos cuando sea necesario.

Producción de informes

IBM Intelligent Operations Center tiene un servicio de generación de informes integrado para que pueda configurar y ejecutar informes con los sucesos y KPI proporcionados por la solución. Puede utilizar este servicio para recopilar y presentar la información más útil de forma regular y actualizada. Este servicio ofrece todas las ventajas de los resúmenes personalizados y las presentaciones gráficas.

Usuarios y beneficios

IBM Intelligent Operations Center se ha diseñado para personal involucrado en el control operativo en empresas, departamentos gubernamentales y autoridades locales o municipales: ejecutivos, supervisores y operadores.

La tabla siguiente describe a los usuarios y beneficios asociados con el uso de IBM Intelligent Operations Center.

Tabla 1. Usuarios y beneficios de IBM Intelligent Operations Center

Si es ...	**Este software puede ayudarle a ...**
Director	• Obtener un resumen de nivel ejecutivo de sucesos e incidencias a través de mapas, paneles de control y alertas • Determinar las medidas de resultados empresariales con indicadores clave de rendimiento (KPI) • Identificar y rastrear problemas mediante informes • Dirigir las prioridades y la implementación de políticas basándose en los datos proporcionados

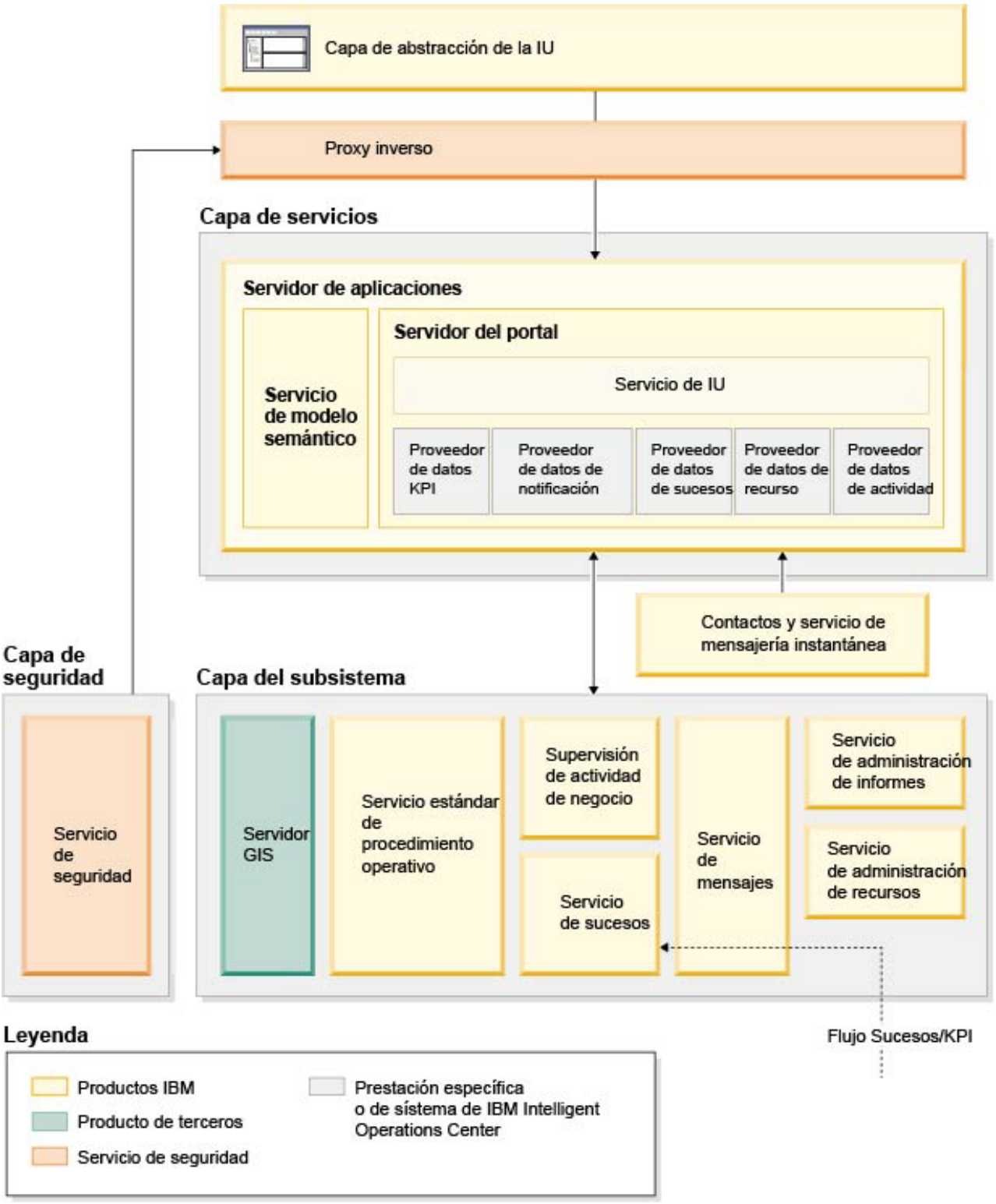
Tabla 1. Usuarios y beneficios de IBM Intelligent Operations Center (continuación)

Si es ...	**Este software puede ayudarle a ...**
Supervisor	• Identificar y actuar sobre los conflictos y los problemas que aparecen en los mapas, paneles de control y alertas • Gestionar sucesos añadiendo nuevos sucesos, editando sucesos existentes, cancelando sucesos y escalando sucesos a incidentes • Proporcionar información sobre recursos y gestionarlos • Almacenar y gestionar la ejecución de los procedimientos y flujos de trabajo asociados con sucesos • Supervisar KPI • Comunicarse rápida y fácilmente sobre asuntos de importancia • Diseñar informes útiles
Operador	• Crear, editar y supervisar los sucesos de estado y las incidencias que se muestra en las listas • Recibir y actualizar estados de las actividades asignadas • Comprobar los recursos disponibles • Ejecutar informes regulares y actualizados • Notificar, actualizar y emitir alertas a los compañeros, responsables o ejecutivos que corresponda • Comunicarse rápida y fácilmente en situaciones de emergencia y otras situaciones que requieran una respuesta
Administrador de usuarios	• Añadir nuevos usuarios y asignarlos a grupos con la autenticación apropiada • Garantizar la seguridad de los datos a través de grupos de autorización basados en roles y categorías con los permiso apropiados • Establecer permisos adecuados a áreas de experiencia y datos necesarios
Administrador del sistema	• Personalizar páginas y portlets para adaptarse a su empresa • Personalizar los sucesos y KPI mostrados según los requisitos de gestión • Crear y publicar sucesos de prueba • Configurar informes y distribución

Componentes

En un nivel superior, la estructura de IBM Intelligent Operations Center se puede dividir en componentes principales, subsistemas y servicios.

El diagrama siguiente muestra una vista de nivel superior de IBM Intelligent Operations Center.



Capa de abstracción de la IU

La IBM Intelligent Operations Center proporciona portales basados en la web integrados para la información del suceso, estado general y detalles. La interfaz de usuario (IU) presenta información personalizada en varias vistas preconfiguradas en formatos comunes. Toda la información se muestra a través de paneles de control fáciles de usar.

Capa de seguridad

Todo el acceso a la información está controlado por la capa de seguridad a través de roles organizativos y de categorías de datos. Este control impide el acceso no autorizado mientras permite una fácil gestión de las autorizaciones.

Capa de servicios

La capa de servicios utiliza asistentes comunes y una infraestructura de servicios de IU común para recibir datos de sucesos y pasarlos a través de la gestión de sucesos al sistema de mensajes. Los proveedores de datos de IBM Intelligent Operations Center amplían los servicios de servicios de la IU. Puesto que se puede proporcionar una gran variedad de datos desde los sistemas operativos proporcionados, los datos se normalizan según un modelo de referencia semántico estándar, que proporciona un diccionario común para correlacionar relaciones. Este modelo facilita el análisis de efecto y responde a sucesos sin la necesidad de múltiples traducciones de información. El modelo semántico proporciona acceso a información KPI y jerárquica de dominios subyacentes. Se puede realizare un análisis avanzado en los datos, identificando optimizaciones y predicciones que pueden ayudar a orientar la toma de decisiones y el gobierno.

Capa del subsistema

La solución proporciona una capa de mediación para facilitar el intercambio de información entre la solución y los sistemas operativos de dominios subyacentes. Se pueden proporcionar datos de diversas fuentes configurables a través de pasarelas a la capa del subsistema, que puede generar alertas, KPI y sucesos. Esta capa de integración permite la comunicación bidireccional de mensajes en varios formatos, utilizando estándares abiertos siempre que sea posible. Mediante el uso de las herramientas estándar de la industria para transformar de orígenes al modelo semántico de referencia, no es necesario cambiar los sistemas operativos subyacentes. Los sistemas de emergencia y otras respuestas se pueden conectar a IBM Intelligent Operations Center para obtener flujos de trabajo adecuados.

La estructura de IBM Intelligent Operations Center soporta:

- Un punto central para entender el estado de las operaciones, gestionar sucesos e incidencias, y conectar dominios en el control del centro de operaciones
- Integración con un sistema de información geográfica (GIS), diagrama de mapa de ubicación o plan de correlación de sucesos, incidencias y recursos de forma espacial y visual
- Creación y supervisión de indicadores de rendimiento clave (KPI), que se actualizan como cambios de datos a través de conexiones con sistemas de dominio subyacentes
- Creación y supervisión de procedimientos operativos estándar (SOP) con flujos de trabajo y actividades junto con sucesos
- Alertas que provienen del campo, incluyendo las que requieren respuestas de emergencia o respuestas estándares
- Capacidades de colaboración, a través de un servicio de mensajería instantánea IBM Lotus Sametime
- Creación y distribución o informes actualizados y regulares basados en sucesos o datos KPI
- Modelo de seguridad basado en un rol

Para obtener más información sobre los servicios de sistema de IBM Intelligent Operations Center, consulte el enlace al final del tema.

Conceptos relacionados:

"Servicios del sistema IBM Intelligent Operations Center" en la página 11
Los servidores IBM Intelligent Operations Center proporcionan varios servicios.

Gestión de sucesos

La solución de IBM Intelligent Operations Center se centra en la integración y optimización de información dentro y a través de varios dominios en un concentrador de operaciones central, en tiempo real y durante largos periodos de tiempo. La gestión de datos de suceso permite que IBM Intelligent Operations Center asimile datos desde varios sistemas para realizar predicciones constantemente y reaccionar ante sucesos y tendencias importantes.

Los mensajes de sucesos son elementos de datos autocontenidos que contienen información básica pero completa a la que los destinatarios pueden responder. Los mensajes de sucesos están colocados en colas por IBM Intelligent Operations Center y los procesa el motor de gestión de sucesos.

Los sucesos entran en IBM Intelligent Operations Center de formas diferentes según la naturaleza de las operaciones y de los dominios en el concentrador de operaciones central. Algunos ejemplos de formas de suceso son: desencadenadores, umbrales, sucesos complejos y sucesos generados manualmente.

Los desencadenadores son sucesos generados por algo que sucede y que generalmente requiere que el destinatario lleve a cabo una acción. Ejemplos de desencadenadores son:

- Alarmas de humo o de incendio que suenan
- Sistemas de tecnología de la información que dejan de funcionar
- Detectores de intrusión activados
- Sucesos naturales recogidos por sensores, como temblores de tierra

El IBM Intelligent Operations Center puede recibir información sobre tales sucesos desde sistemas externos y convertirlos en alertas para los destinatarios. En general, es probable que la disminución de indicadores de nivel se resuma y pase a IBM Intelligent Operations Center si merecen una atención mayor. Por ejemplo, es posible que no se informe de todos los incendios como sucesos. Sin embargo, un incendio que implique a varias divisiones del servicio de incendios y a expertos de protección ambiental, debido a materiales peligrosos, merezca informar al centro de operaciones.

Los sucesos de umbrales le ayudan a determinar cuando las medidas obtenidas desde un sensor u otra fuente se han salido del rango normal. Los sucesos de umbral básico son comparaciones que comparan dos o más medidas e informan de una tendencia. Los sucesos de umbral más sofisticados pueden comparar medidas en un umbral creado por información histórica. Ejemplos de sucesos de umbral son:

- Alarmas de temperatura alta o baja
- Niveles de agua altos y bajos
- Estándares medioambientales de infracciones de pureza del agua y de calidad del aire
- Consumo de alimentación excesivo

El IBM Intelligent Operations Center puede gestionar esos sucesos en forma de indicadores clave de rendimiento (KPI).

Los sucesos complejos llevan reúnen información desde varios sistemas para determinar si se debe informar de un grupo de sucesos relacionados. Por ejemplo, la autorizada del peaje de carretera recibe un suceso desencadenador desde su sistema de supervisión que indica que el enlace informático para la autorización de tarjetas de crédito está inactivo, seguido poco después de un suceso de umbral del sistema financiero avisando de que están cerca del límite de crédito para pagos no autorizados. La combinación de estos dos problemas es mucho más seria que cualquiera de ellos solo, así que se genera un suceso complejo para aumentar la conciencia y coordenar una resolución.

Los sucesos que se entraron manualmente son especialmente importantes para las ciudades. Algunos de ellos se observan como incidencias, como los crímenes y accidentes de tráfico. Otros ejemplos de sucesos entrados manualmente son los generados a partir de llamadas de emergencia de ciudadanos, desde informes realizados por funcionarios de la ciudad o desde el sistema de gestión que informa sobre el estado de la ciudad. Los tipos de sucesos más comunes entrados manualmente son:

- Avisos de tiempo graves
- Denuncias de delitos
- Incendios
- Incidencias en el tráfico por carretera – accidentes, congestión, cargas inusuales
- Sucesos próximos – conciertos de rock, carreras de coches, desfiles

El procesamiento de sucesos complejos permite a la ciudad identificar fácilmente excepciones para los sistemas de la ciudad, ocasionalmente para identificar tendencias a partir de datos no relacionados y para predecir futuros problemas.

Novedades en la versión 1.5

IBM Intelligent Operations Center 1.5 introduce nuevas funciones de gran utilidad para administradores y usuarios.

Novedades para el usuario

Con IBM Intelligent Operations Center 1.5 podrá gestionar recursos y actividades asociados con un suceso.

Gestión de recursos e interacción con mapas de ubicación

En el nuevo Mapa de ubicación y los portlets de Mapa mejorados, podrá:

- Acceder a los recursos disponibles próximos a un suceso según un mapa geográfico.
- Trabajar con un tipo de mapa nuevo, un mapa de ubicación, con áreas interactivas definidas. Por ejemplo, un mapa de ubicación se puede basar en un plan de rutas para un sistema de transporte.
- Ver más de un suceso en clúster en la misma ubicación en un mapa.

Para obtener más información sobre el portlet Mapa de ubicación y los portlets mejoradosMapa y Detalles, siga los enlaces situados al final de este tema.

Seguimiento del estado de las actividades asociadas con sucesos

En el nuevo portlet de Mis actividades, podrá:

- Ver las tareas abiertas para su grupo asociadas con un procedimiento y un suceso.
- Ver el estado de las tareas que tiene asignadas.
- Cambiar el estado de las tareas asignadas.

Para obtener más información sobre el portlet Mis actividades, siga el enlace situado al final de este tema.

Producción de informes

En el nuevo portlet de Informes , podrá:

- Ver hasta seis informes de sucesos como gráficos.
- Crear informes personalizados basándose en criterios y datos seleccionados, como informes para sucesos por fecha o intervalo de fecha.

- Copiar una dirección URL de un informe y mostrar el informe en un marco en la parte derecha del portlet.

Para obtener más información sobre el portlet Informes , siga el enlace situado al final de este tema.

Conceptos relacionados:

"Mapa de ubicación" en la página 282
Utilice el Mapa de ubicación portlet para ver los sucesos marcados en un mapa de ubicación. Un mapa de ubicación en IBM Intelligent Operations Center es un mapa o plano con zonas predefinidas para la interacción, por ejemplo, los asientos en un estadio deportivo.

"Mapa" en la página 285
Uso del portlet Mapa para ver sucesos y recursos en un mapa.

"Detalles" en la página 278
Utilice el portlet Detalles para visualizar, supervisar y gestionar sucesos en IBM Intelligent Operations Center.

"Mis actividades" en la página 290
El portlet Mis actividades muestra una lista dinámica de actividades que son propiedad del grupo del que es miembro el usuario que tiene sesión iniciada en la interfaz.

"Informes " en la página 294
Utilice el portlet Informes para ver un informe de sucesos como gráfico. El portlet proporciona varias opciones para agrupar suceso y puede elegir sucesos por un rango de fechas o por una fecha concreta. Estos informes le ayudan a planificar respuestas para sucesos actuales o futuros.

Novedades para el administrador

Con la versión 1.5, puede personalizar los portlets y diseños de página. También puede configurar procedimientos y flujos de trabajo operativos estándar.

Personalización de portlets

Con las nuevas opciones de configuración de portlet, puede establecer para cada portlet lo siguiente:

- Propiedades específicas de portlets individuales, por ejemplo, establecer el punto central y el nivel de zoom para un mapa
- Propiedades genéricas de los portlets, por ejemplo, establecer la altura del portlet

Para obtener más información sobre la personalización de portlets, siga el enlace situado al final de este tema.

Gestión de sucesos con procedimientos y flujos de trabajo operativos estándar.

Puede definir procedimientos y actividades asociados con sucesos:

- Definir procedimientos de operación estándar en base a un plan de trabajo.
- Crear flujos de trabajo.
- Definir parámetros para la selección de un procedimiento operativo estándar basándose en los parámetros de un suceso.

Para obtener más información sobre la asociación de actividades asociadas con los sucesos, consulte el enlaceprocedimiento operativo estándar situado al final de este tema.

Script y publicación de sucesos

Puede utilizar el nuevo portlet de Script de suceso para crear una lista secuencial de sucesos que se publicará a intervalos de tiempo definidos previamente.

Para obtener más información sobre la realización de scripts y publicación de sucesos, siga el enlace situado al final de este tema.

Comprobación del estado del servicio

Puede utilizar la nueva herramienta de Comprobación de verificación del sistema para comprobar el estado operativo de los servicios de IBM Intelligent Operations Center.

Para obtener más información sobre la herramienta Comprobación de verificación del sistema, siga el enlace situado al final de este tema.

Protocolos de soporte

Ahora IBM Intelligent Operations Center soporta sucesos con protocolos distintos a Protocolo Común de Alertas. Puede:

- Ampliar los tipos enumerados para los sucesos Protocolo Común de Alertas y Protocolo no común de alertas.
- Personalizar los menús emergentes en el portlet Detalles.
- Aceptar los sucesos desde varios dominios para mostrar en los portlets.

Para obtener más información sobre los puntos de integración y protocolos, siga el enlace situado al final de este tema.

Conceptos relacionados:

"Procedimientos operativos estándar" en la página 131
Puede definir procedimientos de operación estándar y actividades para gestionar sucesos que vienen con IBM Intelligent Operations Center. Utilice el portlet Procedimientos operativos estándar para acceder a las aplicaciones procedimiento operativo estándar, matriz de selección del procedimiento de operación estándar y diseñador del flujo de trabajo en Tivoli Service Request Manager.

"Script de suceso" en la página 111
Utilice el portlet Script de suceso para escribir un script para crear una lista secuencial de sucesos que se van a publicar a intervalos de tiempo predefinidos.

"Verificación de componentes" en la página 214
La herramienta Comprobación de verificación del sistema prueba componentes dentro de IBM Intelligent Operations Center para determinar si son accesibles y operativos.

"Protocolos y puntos de integración" en la página 95
Se pueden integrar otros sistemas con la solución a través de los servicios y las políticas de IBM Intelligent Operations Center. Se pueden recibir datos en formato Common Alerting Protocol (CAP) y en otros protocolos.

Tareas relacionadas:

"Personalización de portlets" en la página 149
Como administrador, puede cambiar los valores de portlet para personalizarlo.

Capítulo 2. Instalación y configuración

IBM Intelligent Operations Center proporciona un asistente de despliegue que instala el entorno requerido por el IBM Intelligent Operations Center . Después de desplegar el entorno y el paquete de IBM Intelligent Operations Center , se necesita configuración adicional.

Preparación para la instalación

Antes de implementar IBM Intelligent Operations Center, comprenda la configuración de sistema de IBM Intelligent Operations Center y asegúrese de que se cumplan los requisitos previos del entorno.

Servicios del sistema IBM Intelligent Operations Center

Los servidores IBM Intelligent Operations Center proporcionan varios servicios.

Servicios de analítica
Proporciona servicios de presentación y análisis de datos.

Servidor de aplicaciones
Proporciona servicios de Java Enterprise Edition que admiten el producto.

Seguridad
Proporciona servicios que determinan si un usuario está autorizado a utilizar el sistema y definir sus privilegios dentro del sistema.

Servicios de autorizaciones
Proporciona servicios que determinan los servicios que un usuario está autorizado a usar.

Supervisión empresarial
Proporciona agregación, análisis y presentación del proceso empresarial e información de actividad en tiempo real.

Servidor de mensajería instantánea
Proporciona prestaciones de colaboración en tiempo real para usuarios y aplicaciones.

Servicios de configuración
Gestiona la configuración del producto incluyendo el inventario y la gestión de cambios.

Base de datos
Proporciona el gestor de base de datos para la aplicación y los datos del sistema.

Directorio
Proporciona una correlación entre nombres y valores. Los servicios de datos se utilizan como repositorio para nombres de usuario y contraseñas.

Manejo de sucesos
Recopila, agrega, presenta y gestiona sucesos del sistema.

Servicios de mensajería
Proporciona servicios de flujo de trabajo y mensajes para el producto.

Agentes y servicios de control
Proporciona una actividad de supervisión dentro del producto.

Portal
Proporciona servicios que admiten la interacción del usuario con el producto.

Modelo semántico
Proporciona servicios que permiten aplicaciones para modelar relaciones y objetos del mundo real.

Conceptos relacionados:

"Componentes" en la página 5
En un nivel superior, la estructura de IBM Intelligent Operations Center se puede dividir en componentes principales, subsistemas y servicios.

IBM Intelligent Operations Center Requisitos de hardware

Se necesitan cinco servidores que cumplan los requisitos mínimos para instalar IBM Intelligent Operations Center.

Los servidores deben ser servidores x86 de 64 bits.

Los servidores con requisitos mínimos utilizados por IBM Intelligent Operations Center se muestran enTabla 2. El espacio de disco mínimo recomendado no incluye espacio para particiones de intercambio y arranque.

Tabla 2. Requisitos mínimos de hardware

Recurso	Servidor de aplicaciones	Servidor de sucesos	Servidor de datos	Servidor de gestión	Servidor de instalación
CPU	4	4	4	4	2
Memoria	24 GB	16 GB	16 GB	24 GB	4 GB
Adaptadores de red	1	1	1	1	1
Espacio de disco	113 GB	108 GB	108 GB	108 GB	108 GB
Espacio de disco adicional necesario durante la instalación	90 GB	90 GB	90 GB	90 GB	90 GB

Los requisitos mínimos para los directorios de cada uno de los servidores, excluyendo el espacio requerido para las particiones de intercambio y arranque se muestran en Tabla 3.

Tabla 3. Requisitos de espacio mínimos para cada directorio

Directorio	Espacio mínimo	Notas
`/`	8 GB	
`/opt`	35 GB o 40 GB	Se necesitan 40 GB para servidor de aplicaciones, se necesitan 35 GB para los demás
`/usr`	8 GB	
`/home`	5 GB	
`/tmp`	10 GB	
`/chroot`	1 GB	
`/datahome`	25 GB	
`/loghome`	8 GB	
`/installMedia`	90 GB	Este directorio se puede eliminar después de la instalación.
`/var`	8 GB	

Tareas relacionadas:

"Preparación de los servidores" en la página 17
Antes de instalar IBM Intelligent Operations Center, compruebe que se cumplan los requisitos de configuración. La herramienta de configuración previa verificará que se hayan implementado muchos de estos requisitos.

Información relacionada:

Requisitos del sistema

Requisitos de software prerrequisitos

Antes de instalar IBM Intelligent Operations Center , los servidores deben tener instalado el software adecuado.

IBM Intelligent Operations Center requiere que esté instalado Red Hat Enterprise Linux (RHEL) 5 Server x86-64 Actualización 5 o posterior en todos los servidores. Red Hat Enterprise Linux versión 6 no se admite.

Tareas relacionadas:

"Preparación de los servidores" en la página 17
Antes de instalar IBM Intelligent Operations Center, compruebe que se cumplan los requisitos de configuración. La herramienta de configuración previa verificará que se hayan implementado muchos de estos requisitos.

Información relacionada:

Requisitos del sistema

Navegadores compatibles

La interfaz de soluciones de IBM Intelligent Operations Center soporta varios navegadores. Algunos navegadores pueden utilizarse con limitaciones.

IBM Intelligent Operations Center se ha probado y se admite en los siguientes navegadores:

- Microsoft Internet Explorer 8.x (solo 32 bits)
- Microsoft Internet Explorer 9.x (solo 32 bits)
- Mozilla Firefox 10 ESR

Vista de compatibilidad de Internet Explorer

IBM Intelligent Operations Center no admite la vista de compatibilidad de Internet Explorer 8 o Internet Explorer 9.

Nota: Si observa problemas al crear una nueva página para una interfaz de usuario, puede activar la Vista de compatibilidad temporalmente, para conocer más detalles siga el enlace situado al final de este tema.

Rendimiento de Internet Explorer 8.x

Los usuarios pueden experimentar un rendimiento lento al utilizar Internet Explorer 8.x.

Para evitar este problema, utilice Internet Explorer 9.x o Firefox 10 ESR.

Resolución mínima de pantalla

IBM Intelligent Operations Center esta diseñado para ejecutarse con una resolución mínima de pantalla de 1280 x 800.

Tareas relacionadas:

"No se puede crear una página nueva para la interfaz de usuario" en la página 338
Resuelva los problemas relacionados con la creación de una página nueva si trabaja conMicrosoft Internet Explorer 9.

Empaquetado de soportes

IBM Intelligent Operations Center se puede pedir como un paquete de DVD o se puede obtener a través Passport Advantage .

El número de producto es 5725-D69.

Información relacionada:

Passport Advantage

Descargue los archivos de imagen de IBM Intelligent Operations Center Versión 1.5

Listas de comprobación de instalación

Las listas de comprobación de instalación están disponibles para las dos opciones de instalación diferentes paraIBM Intelligent Operations Center . Estas listas de comprobación proporcionan una visión general de los pasos de instalación y se pueden utilizar para hacer un seguimiento del progreso de la instalación.

Lista de comprobación - instalación utilizando IBM Installation Manager

Utilice la lista de comprobación para rastrear los pasos de instalación al instalar IBM Intelligent Operations Center utilizando IBM Installation Manager.

Acerca de esta tarea

Puede acceder a una versión imprimible de esta lista de comprobación utilizando el enlace relacionado al final de este tema.

Procedimiento

__ 1. Asegúrese de que tiene el hardware necesario.
__ 2. Asegúrese de que el software necesario está instalado en el hardware.
__ 3. Prepare los servidores.
__ 4. Copie el paquete de instalación en el servidor de instalación.
__ 5. Instale el entorno Java Runtime.
__ 6. Instale IBM Installation Manager.
__ 7. Reinicie IBM Installation Manager e instale el paquete **Configurar topología** .
__ 8. Reinicie IBM Installation Manager e instale el paquete **Preparar servidores de destino** . Si este paso se completa satisfactoriamente, salte al paso 9.
__ 9. Reinicie IBM Installation Manager e instale el paquete **Ignorar errores de verificación del sistema** . Al ejecutar IBM Installation Manager después de resolver los errores de verificación del sistema, o después de determinar que la instalación puede continuar, seleccione **Preparar servidores de destino** e **Ignorar errores de verificación del sistema** en la segunda vuelta.
__ 10. Reinicie IBM Installation Manager e instale el paquete **Preparar entorno** .
__ 11. Reiniciar IBM Installation Manager e instalar el paquete **Instalación y configuración de la plataforma - Parte 1** .

Consejo: No seleccione la parte 1 y parte 2 al mismo tiempo. Estos pasos llevarán un tiempo más largo para instalarse. Si se están ejecutando a la vez y hay un fallo, tendrá que volver a ejecutar ambos aunque uno de ellos esté correcto.

Importante: No cierre los servidores antes de que finalicen las fases de instalación. El cierre de los servidores entre fases no se ha comprobado y puede que los resultados sean imprevisibles.

__ 12. Reiniciar IBM Installation Manager e instalar el paquete **Instalación y configuración de la plataforma - Parte 2** .

__ 13. Reinicie IBM Installation Manager e instale el paquete **Instalar herramienta de control de plataforma** .

__ 14. Reinicie IBM Installation Manager e instale el paquete **Instalar herramienta de comprobación de verificación del sistema** .

__ 15. Reinicie todos los servidores de IBM Intelligent Operations Center.

a. Cierre todos los servidores de IBM Intelligent Operations Center con elHerramienta de control de plataforma.

b. Cierre y reinicie todos los servidores desde el sistema operativo.

c. Inicie todos los servidores de IBM Intelligent Operations Center con elHerramienta de control de plataforma.

__ 16. Reinicie IBM Installation Manager e instale el paquete **Instalar aplicación** . Esto se instalará en la aplicación IBM Intelligent Operations Center .

__ 17. Configurar la arquitectura IBM Intelligent Operations Center .

__ a. Configurar los servicios de colaboración si está utilizando IPv6.

__ b. Configurar el inicio de sesión único para servicios de colaboración.

__ c. Instalar y configurar servicios de modelo semántico.

__ d. Configurar Herramienta de control de plataforma.

__ e. Cifre la contraseña administrativa de Tivoli Service Request Manager.

__ f. Establezca el número mínimo de hebras de EventProcessor.

__ g. Cambie el tamaño de la agrupación de hebras predeterminada y del contenedor web.

__ 18. Instalar las demás aplicaciones.

__ 19. Reinicie IBM Installation Manager e instale el paquete **Cyber Hygiene** . Cyber Hygiene proporciona seguridad adicional al sistema IBM Intelligent Operations Center.

Nota: Cyber Hygiene está instalado y se ejecuta en el mismo paso.

__ 20. Configure los usuarios que requieren acceso SSH y contraseñas.

Resultados

La arquitectura IBM Intelligent Operations Center y la aplicación IBM Intelligent Operations Center están instalados y preparados para su uso.

Qué hacer a continuación

La debe reunir herramienta se ofrece para recopilar los registros de instalación para ayudar a diagnosticar problemas de instalación.

Conceptos relacionados:

"Descripción general de Cyber Hygiene" en la página 84
La función Cyber Hygiene de IBM Intelligent Operations Center está diseñada para proporcionar servicios que solucionen exposiciones de seguridad potenciales en el sistema instalado.

Información relacionada:

 Versión para imprimir de esta lista de verificación

Lista de comprobación - instalación paso a paso

Utilice esta lista de comprobación para hacer un seguimiento de los pasos de instalación al instalar IBM Intelligent Operations Center utilizando scripts y mandatos.

Acerca de esta tarea

Puede acceder a una versión imprimible de esta lista de comprobación utilizando el enlace relacionado al final de este tema.

Procedimiento

__ 1. Asegúrese de que tiene el hardware necesario.
__ 2. Asegúrese de que el software necesario está instalado en el hardware.
__ 3. Prepare los servidores.
__ 4. Instale el entorno Java Runtime.
__ 5. Copie el paquete de instalación en el servidor de instalación.
__ 6. Desembale y prepare el paquete de instalación.
__ 7. Defina las propiedades de instalación.
__ 8. Defina la topología de la instalación para editar el archivo de propiedades de topología.
__ 9. Genere la contraseña de topología que se enviará para cifrar los archivos clave.
__ 10. Genere el archivo de topología.
__ 11. Ejecute la herramienta de comprobación previa para verificar que el entorno está preparado para instalar IBM Intelligent Operations Center.
__ 12. Configure los valores de seguridad de Linux utilizando la herramienta proporcionada o ejecutando una serie de mandatos.
__ 13. Instale la arquitectura de IBM Intelligent Operations Center . Esto puede hacerse en una o en tres fases. Si se está ejecutando en un entorno virtualizado, la instalación en varias fases le permite crear una instantánea entre las fases de instalación.
    - Instale IBM Intelligent Operations Center en una fase. La instalación puede llevar hasta 14 horas.
    - Instale IBM Intelligent Operations Center en una fase. Las tres fases son:
        a. Copiar los archivos de instalación de servidor de instalación a los servidores de destino. Esta fase puede llevar aproximadamente 2 horas.
        b. Instalar la primera fase de topología. Esta fase lleva aproximadamente 9 horas.
        c. Instalar la segunda fase de topología. Esta fase lleva aproximadamente 3 horas.

    Importante: No cierre los servidores antes de que finalicen las fases de instalación. El cierre de los servidores entre fases no se ha comprobado y puede que los resultados sean imprevisibles.
__ 14. Instalar Herramienta de control de plataforma.
__ 15. Instalar la herramienta Comprobación de verificación del sistema.
__ 16. Verificar que la arquitectura IBM Intelligent Operations Center está instalada correctamente.
__ 17. Configurar la arquitectura IBM Intelligent Operations Center .

__ a. Configurar los servicios de colaboración si está utilizando IPv6.
__ b. Configurar el inicio de sesión único para servicios de colaboración.
__ c. Instalar y configurar servicios de modelo semántico.
__ d. Cifre la contraseña administrativa de Tivoli Service Request Manager.
__ e. Establezca el número mínimo de hebras de EventProcessor.
__ f. Cambie el tamaño de la agrupación de hebras predeterminada y del contenedor web.

__ 18. Instalar la aplicación IBM Intelligent Operations Center .

__ 19. Instalar las demás aplicaciones.

__ 20. Instale y ejecute Cyber Hygiene. Cyber Hygiene proporciona seguridad adicional al sistema IBM Intelligent Operations Center.

Nota: Cyber Hygiene está instalado y se ejecuta en el mismo paso.

__ 21. Configure los usuarios que requieren acceso SSH y contraseñas.

Resultados

La arquitectura IBM Intelligent Operations Center y la aplicación IBM Intelligent Operations Center están instalados y preparados para su uso.

Qué hacer a continuación

La debe reunir herramienta se ofrece para recopilar los registros de instalación para ayudar a diagnosticar problemas de instalación.

Conceptos relacionados:

"Descripción general de Cyber Hygiene" en la página 84
La función Cyber Hygiene de IBM Intelligent Operations Center está diseñada para proporcionar servicios que solucionen exposiciones de seguridad potenciales en el sistema instalado.

Información relacionada:

 Versión para imprimir de esta lista de verificación

Preparación de los servidores

Antes de instalar IBM Intelligent Operations Center, compruebe que se cumplan los requisitos de configuración. La herramienta de configuración previa verificará que se hayan implementado muchos de estos requisitos.

Acerca de esta tarea

Si se ejecuta en un entorno virtual, utilizando una plantilla para estos pasos podrá reducir el tiempo de configuración.

Procedimiento

1. Asegúrese de que los servidores cumplen los requisitos de hardware y software.
2. Establecer redes TCP/IP.
   a. Definir un nombre completo y un nombre de host abreviado utilizando un servidor DNS o por definición en el archivo `/etc/hosts` .
   b. Verifique la configuración TCP/IP. Los servidores están configurados correctamente si las pruebas siguientes se completan correctamente.
      1) El mandato **`hostname -s`** devuelve el nombre de host abreviado definido para el servidor.

2) El mandato **hostname -f** devuelve el nombre de host y el nombre de dominio completos para el servidor.
3) Los resultados de un mandato **ping** o un mandato **ping6** para entornos IPv6, con el nombre de host abreviado para cada servidor, indica que el servidor es accesible.
4) Los resultados de un mandato **ping** o un mandato **ping6** para entornos IPv6, con el nombre completo para cada servidor, indica que el servidor es accesible.

c. Habilite el direccionamiento de bucle de retorno local para cada servidor del archivo `/etc/hosts` .
d. Verifique el direccionamiento de bucle de retorno local. Los servidores están configurados correctamente si las pruebas siguientes se completan correctamente.
1) El mandato **ping -n localhost** devuelve la dirección `127.0.0.1`.
2) El mandato **ping -n localhost.localdomain** devuelve la dirección `127.0.0.1`.
3) El mandato **ping6 -n localhost6** en un entorno IPV6 devuelve la dirección `::1`.
4) El mandato **ping6 -n localhost6.localdomain6** en un entorno IPV6 devuelve la dirección `::1`.
e. Asegúrese de que los puertos requeridos por IBM Intelligent Operations Center están disponibles. Los puertos requeridos por los servidores se muestran en Tabla 4.

Tabla 4. Puertos necesarios para el uso del producto

Servidor	Puertos necesarios para el uso del producto
Aplicación	80, 82, 389, 390, 443, 2814, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 7234, 7276, 7278, 7279, 7280, 7281, 7283, 7284, 7286, 7287, 7288, 7289, 7290, 7291, 7292, 8008, 8880, 8882, 8883, 8885, 8887, 8889, 8890, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9060, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9354, 9356, 9357, 9359, 9361, 9363, 9364, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9443, 9444, 9445, 9446, 9447, 9448, 9449, 9633, 9634, 9635, 9636, 9638, 9640, 9641, 9810, 9811, 9812, 9813, 9814, 9815, 10000, 10001, 10002, 10003, 10004, 10005, 10006, 10007, 10008, 10009, 10010, 10011, 10012, 10013, 10014, 10015, 10016, 10017, 10025, 10026, 10027, 10028, 10029, 10030, 10031, 10032, 10033, 10034, 10035, 10036, 10037, 10038, 10039, 10040, 10041, 10042, 31000, 31001, 31002, 31003, 31004, 31005, 31006, 31007, 31008, 31009, 31010, 31011, 31012, 31013, 31014, 31015, 31016
Suceso	80 82, 84, 389, 390, 1414, 8008, 9060, 9080, 20000, 31000, 31001, 31002, 31003, 31004, 31005, 31006, 31007, 31008, 31009, 31010, 31011, 31012, 31013, 31014, 31015, 31016
Datos	389, 390, 50000, 50001, 50002, 50003, 50004, 50005, 50006, 50007, 50008
Gestión	80, 82, 389, 390, 1098, 1099, 1527, 1918, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 7135, 7136, 7137, 7276, 7278, 7279, 7280, 7282, 7284, 7286, 7287, 7288, 7289, 7290, 7291, 7292, 7293, 8008, 8880, 8882, 8884, 8886, 8888, 8890, 8892, 9043, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9354, 9356, 9358, 9360, 9362, 9364, 9366, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9443, 9444, 9445, 9446, 9447, 9448, 9448, 9449, 9633, 9634, 9635, 9637, 9639, 9641, 9643, 9810, 9811, 9812, 9813, 9814, 9815, 9816, 13100, 13101, 13104, 41001, 50001

f. Asegúrese de que los descriptores de archivo abierto máximos definidos por el parámetro **nofile** del archivo`/etc/security/limits.conf` se establecen en 20480 para los siguientes servidores:
- Servidor de aplicaciones
- Servidor de sucesos
- Servidor de datos
- Servidor de gestión

Para hacerlo, debe añadir las siguientes líneas al archivo `/etc/security/limits.conf`:

```
*   soft   nofile      20480
*   hard   nofile      20480
```

De esta forma se definirá el límite no estricto (predeterminado) del número de líneas abiertas para todos los usuarios a 20480 y el límite hard (máximo) para todos los usuarios a 20480. Quizá desee aumentar el límite estricto en caso de que otras aplicaciones requieran más de 20480 archivos.

g. Añada o actualice el parámetro **net.ipv4.tcp_fin_timeout** en el archivo `/etc/sysctl.conf` a 30 para los servidores siguientes:
   - Servidor de aplicaciones
   - Servidor de sucesos
   - Servidor de datos
   - Servidor de gestión

3. Inhabilite todos los firewalls de Linux.
4. Inhabilite SELinux (Security Enforcing Linux) editando el archivo `/etc/selinux/config` y cambiando `SELINUX` a `disabled`. Después de cambiar la configuración, vuelva a arrancar el servidor.
5. Asegúrese de que todos los servidores tenga el mismo conjunto de fecha y hora como indica el sistema operativo Linux. Se puede utilizar un servicio de sincronización de hora.
6. Habilite el servicio `sshd` en los servidores ejecutando el mandato **/etc/init.d/sshd start**. El servicio tiene que habilitarse con un inicio de sesión raíz con autenticación de contraseña. El puerto TCP/IP 22 tiene que estar configurado en el sistema operativo como puerto de acceso ssh disponible para su uso durante el proceso de instalación. El número de puerto TCP/IP para el acceso ssh de Herramienta de control de plataforma se especifica en el archivo de propiedades de topología. Solo Herramienta de control de plataforma utiliza el puerto configurado.
7. Instale los paquetes Linux en Tabla 5 en cada servidor utilizando el mandato **yum install** *package_name* . Estos paquetes están disponibles desde Red Hat.

Tabla 5. Paquetes Linux opcionales y necesarios para servidores de destino IBM Intelligent Operations Center

Paquete	Servidor de aplicaciones	Servidor de datos	Servidor de sucesos	Servidor de gestión
`compat-libstdc++-33-3*`	necesario	necesario	necesario	necesario
`libXp-1.0.0-8*`	necesario	opcional	necesario	necesario
`libXmu-1*`	necesario	opcional	necesario	necesario
`libXtst-1*`	necesario	opcional	necesario	necesario
`pam-0*`	necesario	opcional	opcional	opcional
`rpm-build-4*`	necesario	opcional	opcional	necesario
`libaio-0*`	necesario	necesario	opcional	necesario
`libstdc++-4*`	necesario	necesario	necesario	necesario
`libXft-2*`	necesario	opcional	opcional	necesario
`compat-db-4*`	necesario	opcional	opcional	necesario
`elfutils-libs-0*`	necesario	opcional	opcional	necesario
`elfutils-0*`	necesario	opcional	opcional	necesario
`libgcc-4*`	necesario	opcional	necesario	opcional
`compat-glibc-2*`	necesario	opcional	necesario	opcional
`openmotif22-2*`	necesario	opcional	necesario	opcional
`audit-libs-1*`	necesario	opcional	opcional	opcional
`glibc-2*`	necesario	opcional	opcional	opcional
`glibc-common-2*`	necesario	opcional	opcional	opcional

Tabla 5. Paquetes Linux opcionales y necesarios para servidores de destino IBM Intelligent Operations Center (continuación)

Paquete	Servidor de aplicaciones	Servidor de datos	Servidor de sucesos	Servidor de gestión
glibc-headers-2*	opcional	necesario	opcional	necesario
glibc-devel-2*	opcional	necesario	opcional	necesario
compat-gcc*	opcional	necesario	opcional	necesario
libXft-2*	opcional	opcional	necesario	opcional
libXpm-3*	opcional	opcional	necesario	opcional
xorg-x11-xauth*	opcional	opcional	necesario	opcional
ksh-*	opcional	opcional	opcional	necesario

Los siguientes mandatos se pueden utilizar para instalar los paquetes necesarios en cada servidor. Si el paquete ya está instalado, no se volverán a instalar.

Servidor de aplicaciones

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* pam-0*
rpm-build-4* libaio-0* libstdc++-4* libXft-2* compat-db-4* elfutils-libs-0*
elfutils-0* libgcc-4* compat-glibc-2* openmotif22-2* audit-libs-1* glibc-2*
glibc-common-2*
```

Servidor de datos

```
yum install compat-libstdc++-33-3* libaio-0* libstdc++-4* glibc-headers-2*
glibc-devel-2* compat-gcc*
```

Servidor de sucesos

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* libstdc++-4*
libgcc-4* compat-glibc-2* openmotif22-2* libXft-2* libXpm-3* xorg-x11-xauth*
```

Servidor de gestión

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* rpm-build-4*
libaio-0* libstdc++-4* libXft-2* compat-db-4* elfutils-libs-0* elfutils-0*
glibc-headers-2* glibc-devel-2* compat-gcc* ksh-*
```

8. Asegúrese de Java 1.6 no está instalado en ninguno de los servidores:
   - Servidor de instalación
   - Servidor de aplicaciones
   - Servidor de sucesos
   - Servidor de datos
   - Servidor de gestión

Conceptos relacionados:

"Requisitos de software prerrequisitos" en la página 13
Antes de instalar IBM Intelligent Operations Center , los servidores deben tener instalado el software adecuado.

"IBM Intelligent Operations Center Requisitos de hardware" en la página 12
Se necesitan cinco servidores que cumplan los requisitos mínimos para instalar IBM Intelligent Operations Center.

Tareas relacionadas:

"Instalación de IBM Intelligent Operations Center utilizando Installation Manager" en la página 26
IBM Intelligent Operations Center puede instalarse utilizando el instalador gráfico proporcionado.

Información relacionada:

http://www.redhat.com/

Red TCP/IP

Antes de instalar IBM Intelligent Operations Center, la red TCP/IP entre los servidores tienen que estar correctamente configuradas.

Todos los servidores, incluyendo servidor de instalación, utilizado por IBM Intelligent Operations Center tienen que estar configurados con un nombre de host abreviado y un nombre de host completo. Los nombres de host tiene que resolverse en cada uno de los servidores para la dirección IP correcta. La configuración puede llevarse a cabo utilizando un servidor DNS o añadiendo definiciones al archivo `/etc/hosts` .

El nombre de host completo para cada servidor tiene que tener al menos tres componentes. Por ejemplo: `myhost.mydomain.com` donde el dominio de nivel superior es un dominio de Internet de nivel superior estándar.

Importante: Los nombres de host abreviados y los nombres de host completos tienen que estar todos en minúscula o mayúscula según corresponda. Por ejemplo, MyCompany.MyDomain.com no se puede especificar como mycompany.mydomain.com.

IBM Intelligent Operations Center admite la red IPv6, pero IPv4 también se tiene que instalar y configurar. Las direcciones IPv4 no tienen que asignarse a servidores, pero tiene que habilitarse la dirección de bucle de retorno IPv4 (`127.0.0.1`) y el nombre de host `localhost` debe resolverse a `127.0.0.1`.

Los cambios de configuración se muestran en Tabla 6 en la página 22. Estas son las directrices para configurar la red TCP/IP en IBM Intelligent Operations Center servidor de instalación y los servidores de destino editando los archivos de configuración de red Linux. Las notas de configuración en Tabla 6 en la página 22 son únicamente directrices. Cualquier configuración conforme a los requisitos descritos anteriormente debería funcionar.

Tabla 6. Directrices de configuración de TCP/IP

Archivo	Notas

`/etc/hosts`	El archivo `hosts` resuelve los nombres de TCP/IP para la dirección IP. Si la configuración no tiene un servidor DNS, todos los servidores, sus direcciones IP, nombres de host abreviados y nombres de host completos tienen que estar definidos en este archivo. Las direcciones de bucle de retorno local y los nombres de host también se definen en este archivo.
	
	Si se está utilizando un servidor DNS, los host que resuelve DNS no tienen que estar incluidos en este archivo.
	Importante: Al utilizar IPv4, la dirección de bucle de retorno local `127.0.0.1` tiene que correlacionarse con los nombres de host `localhost` y`localhost.localdomain` .
	
	A continuación, tiene un archivo `/etc/hosts` de ejemplo usando direcciones IPv4.
	`# local loopback definitions -- do not remove`
	`# or alter these!`
	`127.0.0.1 localhost.localdomain localhost`
	`# use the following if IPv6 is enabled in your`
	`# network definitions`
	`::1 localhost6.localdomain localhost6`
	
	`# installation server`
	`192.168.0.205 IOC15Install.IOC15.com IOC15Install`
	
	`# target runtime servers`
	`192.168.0.211 IOC15App.IOC15.com IOC15App`
	`192.168.0.212 IOC15Event.IOC15.com IOC15Event`
	`192.168.0.213 IOC15DB.IOC15.com IOC15DB`
	`192.168.0.214 IOC15Mgmt.IOC15.com IOC15Mgmt`
	
	Utilice la notación de dirección IPv6 para asignar direcciones IPv6 estáticas.
	
	Ambas direcciones IPv6 y IPv4 se pueden definir en el mismo servidor.

Tabla 6. Directrices de configuración de TCP/IP (continuación)

Archivo	Notas
/etc/sysconfig/network-scripts/ifcfg-*nombre_adaptador*	El archivo ifcfg-*adapter_name* define los valores de red básicos para el adaptador de red especificado. El nombre de Linux asignado para el adaptador de red se especifica por *nombre_adaptador*. El valor típico para *nombre_adaptador* es eth0 pero puede ser diferente para su entorno. Para la red IPv4, se tienen que definir los siguientes parámetros. **IPADDR** Especifique la dirección IP IPv4 del servidor que se está configurando. **NETMASK** Especifique la máscara de red IPv4 del servidor que se está configurando. **GATEWAY** Especifique la dirección IP de red IPv4 predeterminada del servidor que se está configurando. **BOOTPROTO** Si se está utilizando la dirección IP estática, especifique none. **NM_CONTROLLED** Especifique no para inhabilitar el servicio de gestión de red desde el archivo ifcfg-*adapter_name* modificado. **ONBOOT** Especifique yes para iniciar el adaptador automáticamente. **IPV6INIT** Especifique yes si el adaptador va a utilizar la red IPv6. **IPV6ADDR** Especifique la dirección IP del servidor IPv6 si se especifica IPV6INIT=yes . **IPV6_DEFAULTGW** Especifique la dirección IP de pasarela de red de servidor IPv6 predeterminada si se especifica IPV6INIT=yes .
/etc/sysconfig/network	El archivo network especifica parámetros de red generales. Para la red IPv4, se tienen que definir los siguientes parámetros: **NETWORKING** Especifique yes para habilitar la red IPv4. **NETWORKING_IPV6** Especifique yes si también desea la red IPv6. **HOSTNAME** Especifique el nombre host abreviado del servidor.

Tabla 6. Directrices de configuración de TCP/IP (continuación)

Archivo	Notas

`/etc/resolv.conf`	Se utiliza el archivo `resolv.conf` para definir servidores DNS para la red y un dominio de búsqueda predeterminado. Si no se están utilizando servidores DNS, este archivo tiene que estar vacío.
	
	Si se utiliza un servidor DNS, `resolv.conf` debe contener las siguientes líneas:
	`search` *`domain_name`*
	`nameserver` *`first_DNS_server`*
	`nameserver` *`second_DNS_server`*
	
	Por ejemplo:
	`search yourcompany.com`
	`nameserver 10.75.20.10`
	`nameserver 10.75.20.11`
	
	El valor `search` especifica el dominio de búsqueda predeterminado. El primer valor `nameserver` es la dirección IP del servidor DNS. Se puede utilizar un segundo valor `nameserver` para especificar un servidor DNS secundario. La segunda especificación de `nameserver` es opcional.

`/etc/modprobe.conf`	El archivo `modprobe.conf` define las opciones de configuración de los módulos cargados en el sistema.
	
	Es posible que la red IPv6 requiera que se comenten las siguientes líneas y que se vuelva a arrancar el servidor:
	`alias ipv6 off`
	`options ipv6 disable=1`

Cuando está configurado correctamente, cada servidor debe pasar las siguientes pruebas satisfactoriamente:

1. El mandato **`hostname -s`** devuelve el nombre de host abreviado definido para el servidor.
2. El mandato **`hostname -f`** devuelve el nombre de host y el nombre de dominio completos para el servidor.
3. Los resultados de un mandato **`ping`** o un mandato **`ping6`** para entornos IPv6, con el nombre de host abreviado para cada servidor, indica que el servidor es accesible.
4. Los resultados de un mandato **`ping`** o un mandato **`ping6`** para entornos IPv6, con el nombre completo para cada servidor, indica que el servidor es accesible.

Tareas relacionadas:

"Preparación de los servidores" en la página 17
Antes de instalar IBM Intelligent Operations Center, compruebe que se cumplan los requisitos de configuración. La herramienta de configuración previa verificará que se hayan implementado muchos de estos requisitos.

"La red IPv6 no se inicia" en la página 338
Si la red IPv6 no se inicia en un servidor, es posible que el archivo `/etc/modprobe.conf` requiera cambios.

"Ejecución de la herramienta de comprobación previa" en la página 43
Antes de cargar los paquetes de instalación al servidor de destino, compruebe que los servidores de destino están preparados para la instalación ejecutando la herramienta de comprobación previa.

Copia del paquete de instalación a servidor de instalación

Copie el paquete de instalación de IBM Intelligent Operations Center a servidor de instalación antes de instalar el producto.

Antes de empezar

Antes de copiar el paquete de instalación aservidor de instalación, asegúrese de todos los servidores se han preparado adecuadamente.

Procedimiento

1. Cree un directorio en servidor de instalación para los archivos de instalación, por ejemplo, `/installHome`.
2. Tome nota de la vía de acceso completa al directorio creado. Por ejemplo, si el directorio creado es `installHome` para el usuario `ibmadmin` , la vía de acceso completa debe ser`/home/ibmadmin/installHome`. Esta vía de acceso de directorio se conoce como *install_home* en otras direcciones de instalación.
3. Para cada DVD físico o imagen ISO descargada de Passport Advantage, realice las siguientes acciones.
   a. Cree un directorio donde instalar el DVD. Por ejemplo, ejecute el mandato **mkdir /mnt/ba15**.
   b. Instale el DVD. Por ejemplo, al utilizar una imagen ISO, ejecute el mandato **mount -o loop** *directorio_ISO*/*nombre_archivo_ISO* **/mnt/ba15** donde *directorio_ISO* es la ubicación de la imagen ISO y *nombre_archivo_ISO* es el archivo ISO.
   c. Copie el contenido del DVD en el directorio creado en el paso 1. Por ejemplo, al utilizar una imagen ISO, ejecute el mandato **cp /mnt/ba15/*** *inicio_instalación*.
   d. Desinstale el DVD. Por ejemplo, al utilizar una imagen ISO, ejecute el mandato **umount /mnt/ba15**.
4. Cambie al directorio *inicio_instalación*.
5. Ejecute el mandato **ba15_media_prep.sh combine**. Este mandato se debe ejecutar antes de realizar cualquier otro paso de instalación.

   Nota: Si su directorio *install_home* es distinto a `/installMedia`, edite el archivo`ba15_media_prep.sh` y cambie el valor de `MEDIA_BASE` por su directorio *install_home* designado antes de ejecutar el script. Este mandato combina archivos que están divididos en los DVD o en las imágenes ISO.

Conceptos relacionados:

"Ubicación del soporte de instalación" en la página 31
El IBM Installation Manager permite al instalador especificar dónde están ubicados los paquetes de instalación durante la instalación de IBM Intelligent Operations Center.

Tareas relacionadas:

"Instalación de IBM Intelligent Operations Center utilizando Installation Manager"
IBM Intelligent Operations Center puede instalarse utilizando el instalador gráfico proporcionado.

"Instalación del entorno de tiempo de ejecución Java"
El entorno de ejecución Java 6 debe estar instalado en servidor de instalación antes de instalar IBM Intelligent Operations Center.

Instalación del entorno de tiempo de ejecución Java

El entorno de ejecución Java 6 debe estar instalado en servidor de instalación antes de instalar IBM Intelligent Operations Center.

Acerca de esta tarea

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Procedimiento

1. Inicie sesión como `root` o cambie a la cuenta root ejecutando el mandato **`su -`** .
2. Cambie al directorio donde se copiaron los archivos de instalación de IBM Intelligent Operations Center .
3. Ejecute el mandato **`yum --nogpgcheck install`** *install_media*`/ibm-java-x86_64-jre-6.0-10.1.x86_64.rpm` .
4. Ejecute el mandato **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`**.
5. Verifique el entorno Java ejecutando el mandato **`echo $JAVA_HOME`** y confirmando que se devuelva `/opt/ibm/java-x86_64-60/jre/`.

Tareas relacionadas:

"Copia del paquete de instalación a servidor de instalación" en la página 25
Copie el paquete de instalación de IBM Intelligent Operations Center a servidor de instalación antes de instalar el producto.

"Configuración del Herramienta de control de plataforma" en la página 60
Después de instalar IBM Intelligent Operations Center, si ha instalado un JRE de Java™ diferente del proporcionado con IBM Intelligent Operations Center tiene que definir la ubicación de JRE utilizado por Herramienta de control de plataforma.

"Instalación de IBM Intelligent Operations Center utilizando Installation Manager"
IBM Intelligent Operations Center puede instalarse utilizando el instalador gráfico proporcionado.

Instalación de IBM Intelligent Operations Center utilizando Installation Manager

IBM Intelligent Operations Center puede instalarse utilizando el instalador gráfico proporcionado.

Antes de empezar

El paquete de producto tiene que copiarse en servidor de instalación en el directorio *install-home* antes de los pasos siguientes.

Acerca de esta tarea

Se muestra un indicador de progreso durante la instalación. Sin embargo, dado que las tareas de instalación se están ejecutando de forma remota en los servidores de destino, el indicador de progreso no indica el tiempo real que falta para la instalación. “Componentes de instalación” en la página 30 proporciona el tiempo de instalación estimado para cada componente.

Si desea cancelar la instalación en cualquier momento, pulse **Cancelar** en la interfaz de usuario IBM Installation Manager .

Importante: No ejecute el mandato **launchpad.sh** después de haber instalado correctamente el primer componente. No se le dará la opción de modificar la instalación. Utilice el mandato **/opt/IBM/InstallationManager/eclipse/IBMIM** para reiniciar el instalador en lugar de hacer lo indicado en el paso 24 en la página 28.

Procedimiento

1. Ejecute el mandato **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
2. Extraiga el archivo BA_1.5_GUI_Installer_Lite_Launchpad.zip en *inicio_instalación*.
3. Inicie el launchpad de instalación ejecutando el mandato *inicio_instalación***/launchpad.sh**.
4. Instale IBM Installation Manager.
   a. Pulse **Instalar gestor de instalación de IBM**.
   b. Pulse **Siguiente**.
   c. Lea la información de la licencia.
   d. Si acepta los términos de licencia, seleccione Acepto los términos del acuerdo de licencia y pulse **Siguiente**. La instalación continuará.
   e. Si está de acuerdo con los términos de licencia, seleccione Acepto los términos del acuerdo de licencia y, a continuación, pulse **Siguiente**. La instalación terminará.
   f. Seleccione dónde se instalará IBM Installation Manager .
   g. Pulse **Siguiente**.
   h. Pulse **Instalar**.
   i. Reinicie el IBM Installation Manager.

   IBM Installation Manager está instalado.
5. Una vez esté instalado IBM Installation Manager , IBM Installation Manager tiene que cerrarse y reiniciarse. Al iniciar IBM Installation Manager desde el launchpad, se elegirá el archivo de topología para IBM Intelligent Operations Center.
6. Pulse **Instalación de IBM Intelligent Operations Center**.
7. Seleccione el paquete IBM Intelligent Operations Center - versión 1.5 .
8. Pulse **Siguiente**.
9. Lea la información de la licencia.
   a. Si acepta los términos de licencia, seleccione Acepto los términos del acuerdo de licencia y pulse **Siguiente**. La instalación continuará.
   b. Si está de acuerdo con los términos de licencia, seleccione Acepto los términos del acuerdo de licencia y, a continuación, pulse **Siguiente**. La instalación terminará.
10. Especifique Directorio de recurso compartido para la instalación. Este directorio se utilizará en cualquier momento que utilice IBM Installation Manager para instalar productos utilizando servidor de instalación. Asegúrese de especificar una unidad con el mayor espacio disponible en el servidor.
11. Pulse **Siguiente**.
12. Cree un nuevo grupo de paquetes seleccionando Crear un nuevo grupo de paquetes. Seleccione IBM Intelligent Operations Center.

13. Especifique el nombre del Directorio de instalación. Se creará el Directorio de instalación . El instalador creará subdirectorios bajo este directorio según sea necesario.
14. En Selección de arquitectura, seleccione 64 bits.
15. Pulse **Siguiente**.
16. Anule la selección de todas las opciones.
17. Seleccione **Configurar topología**.
18. Pulse **Siguiente**.
19. Entre las opciones de configuración. Tome nota de todas las contraseñas definidas.
20. Pulse **Siguiente**.
21. Revise las opciones de instalación y pulse **Siguiente** para iniciar la instalación.
22. Una vez se complete la instalación, cierre IBM Installation Manager y el launchpad. No cierre la ventana de terminal donde se inició el launchpad en el paso 3 en la página 27 ya que tiene configurado el entorno JAVA_HOME . Si la ventana de terminal está cerrada, JAVA_HOME debe exportarse de nuevo antes de continuar.
23. Si el valor entrado para la contraseña de topología tiene más de 15 caracteres, haga lo siguiente para definir una contraseña para ITM.ADMIN.USER.PWD que tenga 15 caracteres o menos.
    a. En servidor de instalación edite el archivo*install_home*/ioc/topology/iop_lite_topo.properties donde *install_home* es el directorio donde se copió el paquete de instalación de IBM Intelligent Operations Center .
    b. Cambie el valor definido para ITM.ADMIN.USER.PWD a un valor de 15 caracteres o menos. Esta contraseña se utilizará al iniciar sesión en el usuario sysadmin en lugar de la contraseña de topología.
    c. Guarde los cambios.
24. Inicie IBM Installation Manager ejecutando el mandato **/opt/IBM/InstallationManager/eclipse/IBMIM**.
25. Pulse **Modificar** > **Siguiente**.
26. Seleccione **Preparar servidores de destino**.
27. Pulse **Siguiente** > **Modificar**.
28. Si hay errores, revise los archivos de registro en el directorio /var/ibm/InstallationManager/logs/native . Los nombres del archivo de registro comienza con una indicación de fecha y hora que se puede utilizar para correlacionar el registro cuando se ejecute la instalación.
29. Corrija los errores o avisos encontrados en los registros que pertenecen a su sistema y finalice la instalación antes de instalar el siguiente componente. Se pueden ignorar algunos errores y avisos. Por ejemplo, avisos sobre IPv6 si no tiene habilitado IPv6 o si su configuración no está conectada a un Domain Name Service (DNS).
30. Después de corregir los errores, regrese al paso 25. Tendrá la opción de ignorar los errores de comprobación del sistema. Seleccione el siguiente componente de la lista en el paso 26. Continúe el proceso hasta que se haya instalado Cyber Hygiene.

    Importante: No cierre los servidores antes de que finalicen las fases de instalación. El cierre de los servidores entre fases no se ha comprobado y puede que los resultados sean imprevisibles.

    Cyber Hygiene aplica las configuraciones recomendadas para proporcionar seguridad adicional al sistema IBM Intelligent Operations Center. Antes de instalar Cyber Hygiene, complete la configuración posterior a la instalación. Cuando se haya completado la configuración posterior a la instalación, vuelva al paso 24 e instale y ejecute Cyber Hygiene. Se comprueban los componentes instalados correctamente cuando se ejecutóIBM Installation Manager previamente. No desmarque esos componentes o se desinstalarán cuando se ejecute IBM Installation Manager de nuevo.

Si se ejecuta en un entorno virtualizado, tome una instantánea con memoria de todos los servidores después de que se complete correctamente un paso de la instalación y antes de instalar el siguiente componente. Se puede utilizar esta instantánea para reiniciar la instalación en un estado satisfactorio si se produce un error.

Para reducir el tiempo que Cyber Hygiene invierte en el análisis y la remediación, desmonte el sistema de archivos que no se necesita para la seguridad. Por ejemplo, los directorios *install_media*de cada uno de los servidores se pueden suprimir después de que se completen todos los pasos de la instalación. Estos directorios se pueden suprimir o desmontar antes de ejecutar Cyber Hygiene.

Nota: Cyber Hygiene está instalado y se ejecuta en el mismo paso.

Cyber Hygiene debe ser el último paso antes de mover el sistema a estado de producción o cuando el sistema debe abordar prácticas de seguridad recomendadas. Todas las aplicaciones y soluciones deben estar instaladas y configuradas antes de ejecutar Cyber Hygiene para que se puedan aplicar análisis y remediaciones en el sistema final.

Los cambios aplicados al sistema por Cyber Hygiene pueden causar problemas con otras aplicaciones y soluciones. Por ejemplo, es posible que otras aplicaciones y soluciones tengan requisitos sobre el entorno Linux que no están de acuerdo con las buenas prácticas de seguridad. Una aplicación o solución puede requerir que el sistema esté iniciado como usuario `root` para instalarse o ejecutarse. En este caso, es posible que algunos de los cambios de Cyber Hygiene sean temporales o permanentes u otra solución encontrada por el proveedor de la aplicación o solución.

Después de haber aplicado los cambios de Cyber Hygiene, no hay ningún método automatizado para cambiarlos. Todos los cambios deben realizarse por medio de actualizaciones manuales al sistema operativo Linux o cambiando los permisos del directorio o archivo.

Conceptos relacionados:

"Eliminación de los servicios de instalación desde el sistema de producción" en la página 68
Tras instalar IBM Intelligent Operations Center, los servicios de instalación se pueden eliminar de los servidores del sistema de producción. Se recomienda conservar servidor de instalación ya que algunos de sus servicios podrían ser necesarios en actividades de mantenimiento.

"Configuración posterior a la instalación de IBM Intelligent Operations Center" en la página 53
Después de instalar la arquitectura de IBM Intelligent Operations Center utilizando el gestor de instalación o el paso a paso, se tienen que realizar varios pasos de configuración posterior a la instalación para completarla.

"Descripción general de Cyber Hygiene" en la página 84
La función Cyber Hygiene de IBM Intelligent Operations Center está diseñada para proporcionar servicios que solucionen exposiciones de seguridad potenciales en el sistema instalado.

Tareas relacionadas:

"Preparación de los servidores" en la página 17
Antes de instalar IBM Intelligent Operations Center, compruebe que se cumplan los requisitos de configuración. La herramienta de configuración previa verificará que se hayan implementado muchos de estos requisitos.

"Verificación de la instalación" en la página 52
Después de instalar IBM Intelligent Operations Center, verifique que el producto se ha instalado correctamente.

"Copia del paquete de instalación a servidor de instalación" en la página 25
Copie el paquete de instalación de IBM Intelligent Operations Center a servidor de instalación antes de instalar el producto.

"Instalación del entorno de tiempo de ejecución Java" en la página 26
El entorno de ejecución Java 6 debe estar instalado en servidor de instalación antes de instalar IBM Intelligent Operations Center.

Componentes de instalación

IBM Intelligent Operations Center está instalado como siete componentes.

Tabla 7. Componentes de instalación de IBM Intelligent Operations Center

Componente	Tiempo estimado de instalación	¿Qué se instala?
Preparar instalación	Control previo: 10 minutos Carga: 2 horas	El entorno de servidor está comprobando su cumple los requisitos mínimos y se están copiando los archivos necesarios para la instalación en los servidores de destino.
Preparar entorno	10 minutos	Actualiza los archivos `/etc/sudoers` y `~/.ssh/known_hosts` según sea necesario paraIBM Intelligent Operations Center
Instalar y configurar la plataforma	Fase 1: 12 horas Fase 2: 3 horas	Se instala la plataforma necesaria en los servidores de destino. La instalación se realiza en dos fases.
Herramienta de control de la plataforma	10 minutos	Herramientas necesarias para iniciar, detener y consultar el estado de los servidores IBM Intelligent Operations Center que están instalados en el servidor de gestión.
Plataforma Comprobación de verificación del sistema	15 minutos	Herramientas utilizadas para determinar si están instaladas las prestaciones clave de la plataforma en el servidor de aplicaciones.
Aplicación	3 horas	La aplicación IBM Intelligent Operations Center está instalada en los servidores de destino.

Tabla 7. Componentes de instalación de IBM Intelligent Operations Center (continuación)

Componente	Tiempo estimado de instalación	¿Qué se instala?
Ciberhigiene	hasta 1,5 horas	Las capacidades para mitigar y remediar exposiciones de seguridad de Cyber conocidas están instaladas en los servidores de destino. El tiempo de proceso se determina por la velocidad del hardware y si hay archivos extra no necesarios en los servidores de destino.

Opciones de configuración

La IBM Installation Manager permite al instalador para especificar las opciones de configuración durante la instalación de IBM Intelligent Operations Center .

Contraseña de topología

La IBM Installation Manager permite al instalador especificar las contraseñas que se utilizarán con la IBM Intelligent Operations Center.

El instalador puede especificar las contraseñas mostradas en Tabla 8.

Tabla 8. Contraseñas de IBM Intelligent Operations Center

Contraseña	Descripción
Contraseña de topología	La contraseña de topología es la contraseña utilizada para todas las cuentas creadas por el instalador IBM Intelligent Operations Center excepto las contraseñas solicitadas específicamente durante el proceso de instalación y la contraseña `iicsystemuser` definida como `passw0rd` que no se puede cambiar. La contraseña de topología también protege las claves secretas creadas por el mandato **`createSecretKey`** . La contraseña de la cuenta no puede superar los 15 caracteres. Si la contraseña de topología supera los 15 caracteres de longitud, se deberán realizar pasos de configuración especiales para volver a definir la contraseña de esta cuenta.
Contraseña del usuario administrador	Contraseña del administrador establecida para el usuario `ibmadmin` de Linux. Herramienta de control de plataforma utiliza este usuario al gestionar los componentes del servidor de destino.
Inicialización de cifrado	El valor de inicialización de cifrado se utiliza para cifrar contraseñas de usuario y otros datos sensibles dentro de la base de datos. La inicialización de cifrado debe tener de un valor de 12 a 1016 caracteres ASCII imprimibles. Se debe utilizar una cadena fuerte. Por ejemplo, una cadena larga consta de letras en mayúsculas y minúsculas, números y caracteres especiales sin palabras o frases comunes.
Valor salt de cifrado	El valor salt de cifrado se utiliza para cifrar contraseñas de usuario y otros datos sensibles dentro de la base de datos. El valor salt de cifrado debe tener un valor de 12 caracteres ASCII imprimibles entre 33 y 126 códigos de punto.

Ubicación del soporte de instalación

El IBM Installation Manager permite al instalador especificar dónde están ubicados los paquetes de instalación durante la instalación de IBM Intelligent Operations Center.

El instalador puede especificar los directorios de instalación mostrados en Tabla 9 en la página 32.

Tabla 9. Directorios de instalación de IBM Intelligent Operations Center

Directorio	Descripción	Valor recomendado
Directorio base de imagen local	El nombre del directorio en el servidor de instalación que contiene los archivos de instalación de IBM Intelligent Operations Center. Este es el directorio en el que los archivo de soporte de instalación se han copiado antes de ejecutar la herramienta de instalación. Este directorio se conoce como *soporte_instalación* en otras instrucciones de instalación.	`/installMedia`
Directorio temp de imagen local	El directorio del servidor de instalación utilizado para almacenar los archivos temporales durante la instalación.	`/installMedia`
Directorio de copia de seguridad local	Este directorio es solo para uso interno.	`/tmp/loc/backup`
Directorio de imagen remota	El directorio de los servidores de destino en el que se copiarán los paquetes que van a instalarse en ese servidor.	`/installMedia/loc/image`
Directorio de script remoto	El directorio de los servidores de destino en el que se copiarán los scripts de instalación que se van a ejecutar en ese servidor.	`/installMedia/loc/script`

Tareas relacionadas:

"Copia del paquete de instalación a servidor de instalación" en la página 25
Copie el paquete de instalación de IBM Intelligent Operations Center a servidor de instalación antes de instalar el producto.

Ubicación de Servidor de datos

El IBM Installation Manager permite al instalador definir la conexión a servidor de datos durante la instalación de IBM Intelligent Operations Center.

El instalador puede especificar las opciones de conexión de servidor de datos mostradas en Tabla 10.

Tabla 10. Información de la conexión IBM Intelligent Operations Center Servidor de datos

Opción	Descripción	Valor recomendado
Nombre de host de Servidor de datos	Nombre de host completo para el servidor.	Ninguno. El valor es dependiente de la instalación.
Usuario de Servidor de datos	La cuenta de usuario Linux que se utiliza durante el proceso de instalación.	`raíz`
Contraseña de Servidor de datos	Contraseña para la cuenta especificada en el **Usuario del servidor de datos**.	Ninguno. El valor es dependiente de la instalación.

Para probar la conexión con el servidor, pulse **Probar la conexión**.

Ubicación de Servidor de aplicaciones

El IBM Installation Manager permite al instalador definir la conexión a servidor de aplicaciones durante la instalación de IBM Intelligent Operations Center.

El instalador puede especificar las opciones de conexión de servidor de aplicaciones mostradas en Tabla 11 en la página 33.

Tabla 11. Información de la conexión IBM Intelligent Operations Center servidor de aplicaciones

Opción	Descripción	Valor recomendado
Nombre de host de Servidor de aplicaciones	Nombre de host completo para el servidor.	Ninguno. El valor es dependiente de la instalación.
Usuario de Servidor de aplicaciones	La cuenta de usuario Linux que se utiliza durante el proceso de instalación.	`raíz`
Contraseña de Servidor de aplicaciones	Contraseña para la cuenta especificada en el **Usuario del servidor de aplicaciones**.	Ninguno. El valor es dependiente de la instalación.

Para probar la conexión con el servidor, pulse **Probar la conexión**.

Ubicación de Servidor de sucesos

El IBM Installation Manager permite al instalador definir la conexión a servidor de sucesos durante la instalación de IBM Intelligent Operations Center.

El instalador puede especificar las opciones de conexión de servidor de sucesos mostradas en Tabla 12.

Tabla 12. Información de la conexión IBM Intelligent Operations Center servidor de sucesos

Opción	Descripción	Valor recomendado
Nombre de host de Servidor de sucesos	Nombre de host completo para el servidor.	Ninguno. El valor es dependiente de la instalación.
Usuario de Servidor de sucesos	La cuenta de usuario Linux que se utiliza durante el proceso de instalación.	`raíz`
Contraseña de Servidor de sucesos	Contraseña para la cuenta especificada en el **Usuario del servidor de suceso**.	Ninguno. El valor es dependiente de la instalación.

Para probar la conexión con el servidor, pulse **Probar la conexión**.

Ubicación de Servidor de gestión

El IBM Installation Manager permite al instalador definir la conexión a servidor de gestión durante la instalación de IBM Intelligent Operations Center.

El instalador puede especificar las opciones de conexión de servidor de gestión mostradas en Tabla 13.

Tabla 13. Información de la conexión IBM Intelligent Operations Center servidor de gestión

Opción	Descripción	Valor recomendado
Nombre de host de Servidor de gestión	Nombre de host completo para el servidor.	Ninguno. El valor es dependiente de la instalación.
Usuario de Servidor de gestión	La cuenta de usuario Linux que se utiliza durante el proceso de instalación.	`raíz`
Contraseña de Servidor de gestión	Contraseña para la cuenta especificada en el **Usuario del servidor de gestión**.	Ninguno. El valor es dependiente de la instalación.

Para probar la conexión con el servidor, pulse **Probar la conexión**.

Configuración de Cyber Hygiene

El IBM Installation Manager permite al instalador especificar las opciones requeridas para Cyber Hygiene durante la instalación de IBM Intelligent Operations Center.

El instalador puede especificar las opciones de Cyber Hygiene mostradas en Tabla 14.

Tabla 14. Opciones de Cyber Hygiene de IBM Intelligent Operations Center

Opción	Descripción	Valor recomendado
Contraseña GRUB	Contraseña del gestor de arranque para el sistema. Esta contraseña se utilizará para todos los servidores de destino.	Contraseña especificada por el usuario y coherente con la política de contraseñas de la organización del cliente.
Inhabilitar inicio de sesión raíz remoto	Define si el acceso remoto está inhabilitado para el usuario raíz en todos los servidores de destino.	Se muestra una casilla de verificación con la opción seleccionada. La opción no se puede borrar. El inicio de sesión raíz remoto tiene que inhabilitarse. Se muestra la opción para que el instalador entienda que el inicio de sesión raíz remoto está inhabilitado. Esta configuración no inhabilita el inicio de sesión como `root` desde la consola o cambia a usuario `root` utilizando el mandato**`su`** cuando se inicia sesión en el servidor.

Reinicio de la instalación utilizando el gestor de instalación

Si falla la instalación, se puede reiniciar.

Acerca de esta tarea

Si falla la instalación, la herramienta de instalación revertirá los cambios realizados durante la sesión. Si se seleccionaron varios componentes de instalación, todos los pasos seleccionados se revertirán aunque alguno de los pasos se haya completado correctamente.

Para reiniciar una instalación que ha fallado, haga lo siguiente.

Procedimiento

1. Pulse **Aplicaciones** > **Gestor de instalación de IBM** > **Gestor de instalación de IBM** .
2. Si los componentes no se instalaron correctamente, seleccione **nuevo** para iniciar la instalación desde el principio.
3. Si uno o más componentes se instalaron correctamente, seleccione **modificar** para retener los cambios de instalación existentes. Seleccione el componente o componentes que se van a instalar.

   Nota: Se recomienda utilizar el instalador para instalar los componentes de uno en uno. Esto limitará la retirada de los componentes instalados correctamente si fallaran las posteriores instalaciones de componentes.

Instalación paso a paso de IBM Intelligent Operations Center

IBM Intelligent Operations Center se puede instalar utilizando scripts y pasos de instalación paso a paso.

Preparación del paquete de instalación

Antes de ejecutar los scripts de instalación, se tiene que desempaquetar y preparar el paquete de instalación.

Acerca de esta tarea

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Procedimiento

1. Copie el paquete de instalación en *inicio_instalación*.
2. Extraiga el paquete de instalación.
3. Extraiga `BA_1.5_GUI_Installer_Lite_Launchpad.zip` en el directorio *inicio_instalación*.
4. Cambie al directorio *inicio_instalación*`/repository/native` .
5. Extraiga `com.ibm.iop.ba.lite_1.5.0.9.zip` en el directorio *inicio_instalación*.
6. Extraiga `com.ibm.iop.cat.lite_1.5.0.9.zip` en el directorio *inicio_instalación* .
7. Extraiga `com.ibm.iop.isp.lite_1.5.0.zip` en el directorio *inicio_instalación*`/isp/`.
8. Extraiga `com.ibm.iop.cyber.hygiene.install.lite_1.5.0.zip` en el directorio *inicio_instalación*`/ch`.
9. Ejecute el mandato **cp ../files/com.ibm.iop.cyber.hygiene.scripts.lite_1.5.0.zip [install-home]/ch/install**.
10. Extraiga `com.ibm.iop.ioc.solution.lite_1.5.0.20120807.1518.zip` en el directorio *inicio_instalación*`/ioc/spec` .
11. Extraiga `com.ibm.iop.ioc.topology.lite_1.5.0.20120807.1518.zip` en el directorio *inicio_instalación*`/ioc/topology`.
12. Ejecute el mandato **find** *inicio_instalación* **-name *.sh -exec chmod +x {} \;** .
13. Ejecute el mandato **find** *inicio_instalación* **-name *.sh -exec dos2unix {} \;** .

Verificación del script de instalación

Se puede ejecutar un mandato para mostrar la documentación sobre el instalador. Esto también muestra que el paquete de instalación es operativo.

Acerca de esta tarea

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Procedimiento

1. Inicie sesión como `root` o cambie a la cuenta root ejecutando el mandato **su -** .
2. Ejecute el mandato **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
3. Ejecute el mandato *install_home***/ioc/bin/ba.sh** . Se visualiza la documentación de instalación.

Personalización de las propiedades de instalación

El archivo de propiedades de instalación y los archivos de propiedades de topología proporcionan las definiciones requeridas por los scrips de instalación.

Acerca de esta tarea

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Procedimiento

Opcional: Edite el archivo *install_home*/ioc/resource/custom.properties y cambie los siguientes valores de propiedad si lo desea. Los valores de propiedades del archivo que no están listados en Tabla 15 no deben cambiarse.

Tabla 15. Propiedades de instalación de IBM Intelligent Operations Center

Propiedad	Descripción	Valor predeterminado
image.basedir.local	El nombre del directorio en el servidor de instalación que contiene los archivos de instalación de IBM Intelligent Operations Center. Este es el directorio en el que los archivo de soporte de instalación se han copiado antes de ejecutar la herramienta de instalación. Este directorio se conoce como *soporte_instalación* en otras instrucciones de instalación.	/installMedia
image.tempdir.local	El directorio del servidor de instalación utilizado para almacenar los archivos temporales durante la instalación.	/installMedia
backup.local	Este directorio es solo para uso interno.	/tmp/loc/backup
Unix.image.basedir.remote	El directorio de los servidores de destino en el que se copiarán los paquetes que van a instalarse en ese servidor.	/installMedia/loc/image
Unix.script.basedir.remote	El directorio de los servidores de destino en el que se copiarán los scripts de instalación que se van a ejecutar en ese servidor.	/installMedia/loc/script
connection.timeout	Tiempo de espera (en milisegundos) para una conexión con los servidores de destino antes de fallar	120000
waiting.time	Tiempo de espera (en milisegundos) de espera antes de volver a intentar una conexión fallida	120000
retry.count	Número de veces que se intenta una conexión fallida antes de que falle la instalación	6

Si no se cambian, se utilizarán los valores predeterminados.

Conceptos relacionados:

"Información de contraseña" en la página 39
Las contraseñas para varios ID de usuario utilizadas en la solución IBM Intelligent Operations Center se definen en el archivo de propiedades de topología. Por razones de seguridad, se deben cambiar las contraseñas predeterminadas que vienen con IBM Intelligent Operations Center .

Archivos de topología de instalación

IBM Intelligent Operations Center se ha instalado utilizando un archivo de topología. El archivo de topología es un archivo XML que define los parámetros y los valores utilizados cuando se despliega IBM Intelligent Operations Center en los servidores y define la secuencia utilizada para desplegar los componentes.

Editar el archivo de topología con un editor de texto puede introducir errores. Por esta razón, todas las propiedades personalizables por el cliente se definen en un archivo de propiedades de topología. Un archivo de plantilla de topología proporciona una estructura de topología.

El mandato **parameterizeTopology** adopta los pares de nombre/valor definidos en el archivo de propiedades de topología y la estructura proporcionada por el archivo de plantilla de topología y crea un archivo de topología válido que después se utiliza durante la instalación.

IBM Intelligent Operations Center proporciona los siguientes archivos de topología:

Nombre del archivo	Objetivo
install_home/ioc/resource/custom.properties	Define la ubicación de los soportes de instalación, directorios de trabajo y otras propiedades. Se puede editar el archivo para que cumpla con las necesidades del entorno del cliente.
install_home/ioc/topology/iop_lite_topo.properties	Define las propiedades personalizables por el cliente para el despliegue incluyendo los nombres de host y las contraseñas. Se puede editar el archivo para que cumpla con las necesidades del entorno del cliente.
install_home/ioc/topology/iop_lite_topo.template.xml	Define la estructura de la topología que se va a desplegar. Este archivo utiliza valores definidos en el archivo propiedades. Este archivo no se debe editar.
install_home/ioc/topology/iop_lite_topo.xml	Define la topología que se va a desplegar. El archivo se crea por medio del mandato **parameterizeTopology** que utiliza la información del archivo de plantilla y de propiedades. Bi se debe modificar el archivo a menos que sea necesario para recuperarse de un fallo de instalación.
install_home/ioc/topology/iop_lite_topo.chk	Define las reglas utilizadas por la herramienta de comprobación previa para determinar si los servidores del servicio están configurados correctamente para la instalación de IBM Intelligent Operations Center. Este archivo no se debe editar.

Tareas relacionadas:

"Instalación de Herramienta de control de plataforma" en la página 49
El Herramienta de control de plataforma se utiliza para gestionar el entorno de servidor de IBM Intelligent Operations Center . La herramienta se instalada independiente del producto.

Archivo de propiedades de topología

El archivo de propiedades de topología define las propiedades personalizables por el usuario para el despliegue de IBM Intelligent Operations Center. Edite este archivo para que cumpla los requisitos del entorno del cliente. Las propiedades del archivo de propiedades de topología no documentadas aquí no se deben cambiar.

Después de modificar el archivo de propiedades de topología, guarde una copia en una ubicación segura. El archivo contiene información de seguridad sensible, como los nombres de usuario y contraseñas para el sistema, en texto simple. Si una persona no autorizada tiene acceso a este archivo, tendrá acceso completo al sistema.

El archivo de propiedades de topología se puede utiliza después de la instalación de las siguientes formas:

- Como repositorio de información de contraseña si se olvida una contraseña.
- Como repositorio para contraseñas cuando se cambian en el sistema. El archivo de propiedades de topología modificado se puede utilizar para actualizar las contraseñas utilizadas por Herramienta de control de plataforma.
- Como copia de seguridad de información de instalación si el sistema se tiene que volver a instalar. El archivo de propiedades de topología se puede utilizar sin tener que redefinir todos los parámetros de instalación.

Tareas relacionadas:

"Generación del archivo de topología" en la página 42
Antes de ejecutar los pasos de instalación de IBM Intelligent Operations Center, genere un archivo de topología con los parámetros necesarios para la instalación.

Información del servidor de destino:

La sección SERVERS del archivo de propiedades de topología define las propiedades de los servidores de destino.

Tabla 16 muestra los valores de propiedad de servidor que se pueden especificar en el archivo de propiedades de topología.

Tabla 16. Propiedades de servidor de destino

Propiedad	Descripción
DB.1.HOST	El nombre de host del servidor de datos
DB.1.ACCOUNT.PWD	La contraseña root para servidor de datos
DB.1.SSH_PORT	El número de puerto para el acceso SSH al servidor de datos
APP.1.HOST	El nombre de host del servidor de aplicaciones
APP.1.ACCOUNT.PWD	La contraseña root para servidor de aplicaciones
APP.1.SSH_PORT	El número de puerto para el acceso SSH al servidor de aplicaciones
EVENT.1.HOST	El nombre de host del servidor de sucesos
EVENT.1.ACCOUNT.PWD	La contraseña root para servidor de sucesos
EVENT.1.SSH_PORT	El número de puerto para el acceso SSH al servidor de sucesos
MGMT.1.HOST	El nombre de host del servidor de gestión
MGMT.1.ACCOUNT.PWD	La contraseña root para servidor de gestión
MGMT.1.SSH_PORT	El número de puerto para el acceso SSH al servidor de gestión

Importante: Los valores del nombre de host debe ser nombres de host completos entrados en el caso definido. Por ejemplo, IOC15App.IOC15.com no es igual que ioc15app.ioc15.com.

Se puede configurar un número de puerto ssh para cada servidor. Sin embargo, los números de puerto configurados sólo los pueden utilizar Herramienta de control de plataforma. El puerto 22 debe estar habilitado para el acceso ssh en cada servidor. El puerto 22 es necesario para que IBM Intelligent Operations Center acceda mediante ssh durante la instalación.

Información de servicios de directorio:

El archivo de propiedades de topología define los valores utilizados para cifrar contraseñas de usuario y otros datos sensibles dentro del directorio.

El cifrado se basa en dos valores: LDAP.SEED y LDAP.SALT.

Los valores deben ser caracteres ASCII imprimibles. Los caracteres ASCII imprimibles son caracteres con valores de punto de código de 33 a 126. No se puede utilizar un espacio en blanco.

Tabla 17. Propiedades de los servicios de directorio

Propiedad	Descripción
LDAP.SEED	Una cadena formada como mínimo por 12 caracteres y como máximo por 1016 caracteres ASCII imprimibles, entre 33 y 126 puntos de código. Se debe usar una cadena criptográficamente sólida. Por ejemplo, una cadena larga consta de letras en mayúsculas y minúsculas, números y caracteres especiales sin palabras o frases comunes.
LDAP.SALT	Una cadena formada por 12 caracteres ASCII imprimibles, entre 33 y 126 puntos de código. **Importante:** LDAP.SALT debe tener exactamente 12 caracteres de longitud. Un valor con más o menos caracteres provocará un error en la instalación.

Registre los valores LDAP.SEED y LDAP.SALT fuera del sistema. Se necesitarán los valores si tiene que explotar o replicar entradas de directorio.

Información de contraseña:

Las contraseñas para varios ID de usuario utilizadas en la solución IBM Intelligent Operations Center se definen en el archivo de propiedades de topología. Por razones de seguridad, se deben cambiar las contraseñas predeterminadas que vienen con IBM Intelligent Operations Center .

Las contraseñas sólo pueden contener caracteres alfanuméricos (AZ, az, 0-9). A menos que se indique lo contrario, las contraseñas deben tener 30 caracteres o menos.

Tabla 18. Propiedades de contraseñas

Propiedad	Nombre de usuario asociado	Descripción
LDAP.DB.PWD	dsrdbm01	Base de datos de directorio LDAP
LDAP.ADMIN.DN.PWD	cn=root	Enlace de administrador LDAP
LDAP.BIND.DN.PWD	cn=bind	enlace LDAP
LDAP.PROXY.INSTANCE.PWD	tdsproxy	Instancia del proxy LDAP
LDAP.PROXY.ADMIN.DN.PWD	cn=root	Enlace de administrador de proxy LDAP
LDAP.PROXY.BIND.DN.PWD	cn=bind	Enlace de proxy LDAP
TAM.SECMASTER.PWD	ninguno	Contraseña maestra del servicio de seguridad A este usuario se le otorgan privilegios equivalentes al usuario root en el servidor de destino. A causa del acceso otorgado al usuario, asegúrese de que la contraseña sea un valor largo, diferente de las otras contraseñas y que se conserva en un lugar seguro.

Tabla 18. Propiedades de contraseñas (continuación)

Propiedad	Nombre de usuario asociado	Descripción
TAM.WEBSEAL.ADMIN.PWD	sec_master	Administrador del servicio de seguridad A este usuario se le otorgan privilegios equivalentes al usuario root en el servidor de destino. A causa del acceso otorgado al usuario, asegúrese de que la contraseña sea un valor largo, diferente de las otras contraseñas y que se conserva en un lugar seguro.
WBM.DB.USER.PWD	db2ibm	Base de datos del servicio de supervisión de actividad de negocio
WODM.DB.USER.PWD	db2wodm	Base de datos de servicio de gestión de decisión
WODM.ADMIN.UID.PWD	resAdmin1	Administrador del servicio Decision Management
WODM.DEPLOYER.UID.PWD	resDeployer1	Desplegador de la regla de servicio de Decision Management
WODM.MONITOR.UID.PWD	resMonitor1	Supervisor de servicio de Decision Management
WODM.DB.DC.USER.PWD	wodmdc	Base de datos de la consola de Decision
WODM.rtsAdmin.UID.PWD	rtsAdmin	Administrador de la consola de Decision
WODM.rtsConfig.UID.PWD	rtsConfig	Configuración de la consola Decision
WODM.rtsUser.UID.PWD	rtsUser	Usuario de consola Decision
UDDI.DB.USER.PWD	db2uddi	Base de datos de servicio UDDI
IHS.KEYSTORE.PWD	ninguno	Almacén de claves de servidor HTTP
WAS.ADMIN.ACCOUNT.PWD	waswebadmin	Administrador de servicios de aplicación
WAS.LTPA.PWD	ninguno	Símbolo LTPA
PORTAL.ADMIN.ACCOUNT.PWD	waswebadmin	Administración para la consola de WebSphere Application Server para el servidor WebSphere Portal
PORTAL.ADMIN.UID.PWD	wpsadmin	Administrador para el servidor WebSphere Portal
PORTAL.DB.USER.PWD	db2port1	Base de datos WebSphere Portal
OMNIBUS.ADMIN.ACCOUNT.PWD	netcool	Administrador de servicios de sucesos
IMPACT.WAS.ACCOUNT.PWD	wasadmin	Administrador de servicios de sucesos del sistema
TSRM.WAS.ADMIN.PWD	waswebadmin	Administrador de gestor de solicitud de servicio
TSRM.DB.USER.PWD	máximo	Base de datos del gestor de solicitud de servicio
TSRM.ADMIN.USER.PWD	maxadmin	Administrador de gestor de solicitud de servicio

Tabla 18. Propiedades de contraseñas (continuación)

Propiedad	Nombre de usuario asociado	Descripción
TSRM.REG.USER.PWD	maxreg	Usuario gestor de solicitud de servicio
TSRM.INITADM.USER.PWD	maxintadm	Usuario de integración de gestor de solicitud de servicio
MGMT.WAS.ADMIN.PWD	waswebadmin	Administrador de servicios de aplicación
TEPS.DB.USER.PWD	itmuser	Base de datos de Enterprise Portal
TIM.STORE.PWD	ninguno	Almacén de gestión de identidad
TIM.ADMIN.USER.PWD	waswebadmin	Administrador de gestor de identidad
DOMINO.USER.PWD	notas	Usuario de colaboración
DOMINO.ORG.PWD	IBM	Organización de colaboración
DOMINO.ADMIN.PWD	admin de notas	Administrador de colaboración
DOMINO.ST.ADMIN.PWD	wpsadmin	Administrador de portal de colaboración
DOMINO.ST.BIND.PWD	wpsbind	Enlace LDAP de colaboración
DEFAULT.PWD.DAS	dausr1, dausr2, dausr3, dausr4, dausr5, dausr6, dausr7, dausr8	Servidor administrativo de servicios de base de datos
DEFAULT.PWD.DB2	db2inst1, db2inst2, db2inst3, db2inst4, db2inst5, db2inst6, db2inst7, db2inst8	Servidor de datos de servicios de base de datos
DEFAULT.PWD.IHS	ihsadmin	Servidor HTTP
DEFAULT.PWD.MQM	mqm	Usuario de servicio de mensajería
MQM.CONN.USER.PWD	mqmconn	Conexión de servicios de mensajería
DEFAULT.PWD.TAI	taiuser	Seguridad de servicios de aplicación
ITM.ADMIN.PWD	sysadmin	Administrador de gestión del sistema **Restricción:** La contraseña debe ser de 15 caracteres o menos.
IOP.ADMIN.USER.PWD	ibmadmin	Herramientas de administración del sistema A este usuario se le otorgan privilegios equivalentes al usuario `root` en el servidor de destino. El usuario Herramienta de control de plataforma se ejecuta bajo este nombre de usuario. A causa del acceso otorgado al usuario, asegúrese de que la contraseña sea un valor largo, diferente de las otras contraseñas y que se conserva en un lugar seguro.
IOP.USER.USER.PWD	ibmuser	Usuario general del sistema

Conceptos relacionados:

Capítulo 3, “Asegurar la solución”, en la página 71
La seguridad es importante dentro de IBM Intelligent Operations Center porque la solución es central para las operaciones esenciales. Para garantizar la seguridad, es importante que sea consciente de la configuración predeterminada y de que gestiona usuarios de la solución para proporcionar a todos los usuarios el nivel de acceso correcto.

Tareas relacionadas:

“Personalización de las propiedades de instalación” en la página 35
El archivo de propiedades de instalación y los archivos de propiedades de topología proporcionan las definiciones requeridas por los scrips de instalación.

Referencia relacionada:

“Usuarios de muestra” en la página 73
Durante el despliegue de IBM Intelligent Operations Center, se crean usuarios de muestra.

Creación de la contraseña de topología

La contraseña de topología se utiliza durante el proceso de instalación para cifrar y acceder al archivo que define la topología de solución.

Acerca de esta tarea

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Procedimiento

1. Inicie sesión como `root` o cambie a la cuenta root ejecutando el mandato **`su -`** .
2. Ejecute el mandato **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`**.
3. Cambie al directorio *`inicio_instalación`*`/ioc`.
4. Ejecute el mandato **`bin/ba.sh createSecretKey -p`** *contraseña* donde *contraseña* es la contraseña que se creará para la topología. Este mandato crea el archivo *`install_home`*`/ioc/resource/ioc.keystore` . Este archivo contiene la clave utilizada para cifrar el archivo de propiedades de topología. El archivo `ioc.keystore` también está cifrado con la contraseña especificada en el mandato **`createSecretKey`** . Para cambiar la contraseña y la clave para la instalación, suprima el archivo *`install_home`*`/ioc/resource/ioc.keystore` y, después, vuelva a ejecutar el mandato **`createSecretKey`** . Tome nota de la contraseña para su uso en otros pasos de la instalación.

Tareas relacionadas:

“Generación del archivo de topología”
Antes de ejecutar los pasos de instalación de IBM Intelligent Operations Center, genere un archivo de topología con los parámetros necesarios para la instalación.

Generación del archivo de topología

Antes de ejecutar los pasos de instalación de IBM Intelligent Operations Center, genere un archivo de topología con los parámetros necesarios para la instalación.

Acerca de esta tarea

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Procedimiento

1. Inicie sesión como `root` o cambie a la cuenta root ejecutando el mandato **`su -`** .
2. Ejecute el mandato **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`**.
3. Vaya al directorio *`install_home`*`/ioc/topology` .

4. Edite el archivo `iop_lite_topo.properties` haciendo los cambios necesarios para el entorno.
5. Copie el archivo de la plantilla de topología en el archivo de topología ejecutando el mandato **cp iop_lite_topo.template.xml iop_lite_topo.xml**.
6. Cambie al directorio *inicio_instalación*/ioc.
7. Ejecute el mandato **bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p** *contraseña* donde *contraseña* es la contraseña de topología. Los parámetros definidos en el archivo de propiedades de topología se aplican al archivo de topología.
8. Opcional: Para cifrar contraseñas en el archivo de topología, ejecute el mandato **bin/ba.sh encryptTopology -t iop_lite_topo -p** *contraseña* donde *contraseña* es la contraseña de topología.

   Importante: Sólo se cifrarán las contraseñas del archivo de topología. Las contraseñas de los archivos, por ejemplo del archivo de propiedades de topología, no se cifrarán.

Conceptos relacionados:

"Archivo de propiedades de topología" en la página 37
El archivo de propiedades de topología define las propiedades personalizables por el usuario para el despliegue de IBM Intelligent Operations Center. Edite este archivo para que cumpla los requisitos del entorno del cliente. Las propiedades del archivo de propiedades de topología no documentadas aquí no se deben cambiar.

Tareas relacionadas:

"Creación de la contraseña de topología" en la página 42
La contraseña de topología se utiliza durante el proceso de instalación para cifrar y acceder al archivo que define la topología de solución.

Ejecución de la herramienta de comprobación previa

Antes de cargar los paquetes de instalación al servidor de destino, compruebe que los servidores de destino están preparados para la instalación ejecutando la herramienta de comprobación previa.

Acerca de esta tarea

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Procedimiento

1. Inicie sesión como `root` o cambie a la cuenta root ejecutando el mandato **su -** .
2. Ejecute el mandato **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
3. Cambie al directorio *inicio_instalación*/ioc.
4. Ejecute el mandato **bin/ba.sh precheckTopology -t iop_lite_topo -p** *contraseña* donde *contraseña* es la contraseña de topología. Se mostrarán mensajes para cada prueba de comprobación previa en cada servidor. El estado de cada una de las pruebas será `[Pass]` o `[Fail]`. Una vez se han ejecutado todas las pruebas, se mostrará un resumen de todas las pruebas fallidas.
5. Si hay muchos errores, tome las medidas adecuadas para arreglar el problema y vuelva a ejecutar la comprobación previa hasta que no haya errores.

Resultados

Si se emite el mensaje CHK0101W no hay un servidor de DNS configurado para el entorno, o el servidor de DNS no tiene sus servidores definidos. Esta advertencia se puede ignorar si los servidores se han definido utilizando una dirección IP estática en el archivo `/etc/hosts`.

Conceptos relacionados:

"Red TCP/IP" en la página 21
Antes de instalar IBM Intelligent Operations Center, la red TCP/IP entre los servidores tienen que estar correctamente configuradas.

Configuración de seguridad de Linux

Se debe cambiar la configuración de seguridad de Linux para habilitar Herramienta de control de plataforma.

Se pueden cambiar estos valores ejecutando una serie de mandatos o utilizando un script.

El script realiza los cambios indicados por los mandatos. Si los mandatos no cumplen las necesidades de instalación, o si los procesos de empresa no permiten que se realicen cambios de seguridad utilizando un script, cambie la configuración utilizando mandatos individuales.

Adaptación manual de la configuración de seguridad de Linux

La configuración de seguridad requerida de Linux se puede hacer mediante la ejecución de una serie de mandatos.

Procedimiento

1. En el servidor de instalación, inicie sesión como `root` o ejecute el mandato **`su -`** para conmutar a la cuenta raíz.
2. Realice lo siguiente para habilitar la Herramienta de control de plataforma. Estos pasos deben ejecutarse para cada uno de los servidores de destino siguientes:
   - Servidor de aplicaciones
   - Servidor de datos
   - Servidor de sucesos
   - Servidor de gestión

   a. Ejecute el mandato **`visudo`**. El archivo `/etc/sudoers` se abrirá para su edición.
   b. Escriba la letra `i` para cambiar a la modalidad de inserción, que permite hacer cambios en el archivo.
   c. Localice la siguiente línea:
      ```
      #%wheel ALL=(ALL) NOPASSWD: ALL
      ```
      Y cambie la línea a:
      ```
      %wheel ALL=(ALL) NOPASSWD: ALL
      ```
   d. Añada la siguiente línea al final del archivo:
      ```
      Defaults:%wheel !requiretty
      ```
   e. Pulse Esc. Se sale de la modalidad de inserción.
   f. Escriba `:wq`. Se guarda el archivo.
   g. Ejecute el mandato **`exit`**. El sistema vuelve al inicio de sesión de servidor de instalación.

   Cuando se haya completado para los cuatros servidores, la seguridad de Linux permite a los usuarios del grupo `wheel` utilizar el mandato **`sudo`** para ejecutar mandatos del sistema de forma local o desde una sesión remota.

Tareas relacionadas:

"Adaptación de la configuración de seguridad de Linux con un script"
La configuración de seguridad requerida de Linux se puede hacer mediante la ejecución de un script.

Adaptación de la configuración de seguridad de Linux con un script

La configuración de seguridad requerida de Linux se puede hacer mediante la ejecución de un script.

Acerca de esta tarea

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Procedimiento

1. Cambie al directorio *inicio_instalación*/ioc.
2. Ejecute el mandato **bin/install-prepare-env.sh -d** *inicio_instalación***/ioc -f topology/iop_lite_topo.properties -p** *contraseña* donde *contraseña* es la contraseña de topología.

Tareas relacionadas:

"Adaptación manual de la configuración de seguridad de Linux" en la página 44
La configuración de seguridad requerida de Linux se puede hacer mediante la ejecución de una serie de mandatos.

mandato installTopology

El mandato **installTopology** utiliza la información del archivo de topología para instalar IBM Intelligent Operations Center.

Antes de utilizar el archivo de topología para instalar IBM Intelligent Operations Center, el mandato **installTopology** comprobará que los archivos de instalación se hayan copiado a los servidores de destino. Si no se han copiado los archivos, el mandato **installTopology** copiará los archivos necesarios antes de proceder.

Utilizando el archivo de topología como guía, el mandato **installTopology** instalará cada componente de IBM Intelligent Operations Center y realizará la configuración necesaria. Se mostrarán mensajes durante la instalación que indican el progreso de la instalación.

Si se produce un error durante el procesamiento del mandato **installTopology** , es posible que la instalación se tenga que reiniciar antes de resolver porqué una o más instalaciones de componentes fallaron. Las instalaciones erróneas se indican mediante el estado de instalación del archivo de topología.

Nota: En un entorno virtual, se sugiere que se tomará la instantánea de un entorno antes de ejecutar el mandato **installTopology** y después de cada instalación correcta.

Estado de instalación

El atributo **Status** del archivo de topología indica el estado de instalación de cada componente. Cuando se ejecute el mandato **installTopology**, se realizará la acción indicada en Tabla 19 en función del estado del componente.

Tabla 19. Estado y acciones de instalación

Valor	Estado	Acción installTopology
Nuevo	El componente no se ha instalado.	El estado cambiará a Incierto y se instalará el componente. Cuando el componente se instala correctamente, el estado cambia a Preparado.
Preparado	El componente se instaló correctamente.	La instalación del componente se saltará cuando se ejecute el mandato **installTopology** de nuevo.
Indeterminado	El componente no se ha instalado correctamente o la instalación está en curso.	El componente se instalará. Cuando el componente se instala correctamente, el estado cambia a Preparado.

Opciones para la instalación de componentes de IBM Intelligent Operations Center

La instalación de IBM Intelligent Operations Center puede llevar muchas horas. Debido al tiempo necesario, IBM Intelligent Operations Center se puede instalar en una o múltiples fases.

En una sola fase de instalación, el proceso de instalación se ejecuta hasta que todos los componentes se instalan o se produzca un fallo en la instalación. Si la instalación falla, se debe reiniciar desde el principio.

En una instalación de múltiples fases, el proceso de instalación se divide en tres fases distintas:

uploadTopology
Copia los archivos de instalación desde servidor de instalación a los servidores de destino.

Fase 1 Instala algunos de los componentes de IBM Intelligent Operations Center creando una base para la instalación de componentes que quedan.

Fase 2 Instala los componentes IBM Intelligent Operations Center que quedan.

Al ejecutarse en un entorno virtualizado, se debería tomar una instantánea después de cada fase si se requiere un reinicio.

La fase **uploadTopology** se ejecuta como mandato aparte. Si ya se han copiado los archivos de instalación a los servidores de destino, no se copiarán de nuevo.

La fase o fases que se ejecutarán se deben ejecutar se definen en el archivo de propiedades de topología. Las propiedades **Status.Phase1** y **Status.Phase2** determinan si las fases de instalación se ejecutarán cuando se ejecute el mandato **installTopology** . Si se establecen en New , la fase de ejecutará. Si se establecen en Ready , la fase de saltará.

Instalación de la arquitectura IBM Intelligent Operations Center en una única fase

La arquitectura utilizada con IBM Intelligent Operations Center puede instalarse en una única fase. Si va a instalar en un entorno virtualizado, ejecutar la instalación en una única fase no se le permitirá tomar instantáneas durante el proceso de instalación.

Acerca de esta tarea

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Procedimiento

1. En el servidor de instalación, abra una ventana de terminal e inicie sesión como `root`. Si no se inicia sesión como `root`, cambie e la cuenta `root` utilizando el mandato **su -**.
2. Copie los archivos necesarios para la instalación a los servidores de destino e instale IBM Intelligent Operations Center.
   a. Cambie al directorio *inicio_instalación*`/ioc`.
   b. Ejecute el mandato **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
   c. Ejecute el mandato **bin/ba.sh installTopology -t iop_lite_topo -p** *contraseña*, donde *contraseña* es la contraseña de la topología.

   Se copiarán los archivos necesarios a los servidores de destino y se instalará IBM Intelligent Operations Center .

   Se visualizan mensajes que indican el progreso de la instalación. Los mensajes indican el estado del componente instalado. El estado será uno de los valores siguientes:

   [OK] Componente instalado correctamente.

[Fail]
Se ha encontrado un error en la instalación del componente.

Resultados

El proceso de instalación puede llegar a tardar 14 horas. La arquitectura de IBM Intelligent Operations Center está instalada correctamente cuando todos los mensajes estén completos con un estado `[ OK ]` .

Instalación de la arquitectura IBM Intelligent Operations Center en varias fases

La arquitectura utilizada con IBM Intelligent Operations Center puede instalarse en varias fases. Una instalación en varias fases le permitirá resolver problemas de instalación antes, en lugar de esperar a que se complete todo el proceso de instalación. Si está instalando en un entorno virtualizado, ejecutar la instalación en varios pasos le permitirá tomar instantáneas durante el proceso de instalación.

Acerca de esta tarea

Importante: No cierre los servidores antes de que finalicen las fases de instalación. El cierre de los servidores entre fases no se ha comprobado y puede que los resultados sean imprevisibles.

Procedimiento

1. En el servidor de instalación, abra una ventana de terminal e inicie sesión como `root`. Si no se inicia sesión como `root`, cambie e la cuenta `root` utilizando el mandato **`su -`**.
2. Ejecute el mandato **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`**.
3. Copie los archivos de instalación en los servidores de destino.
   a. Cambie al directorio *`inicio_instalación`*`/ioc`.
   b. Ejecute el mandato **`bin/ba.sh uploadImage -t iop_lite_topo -threadCount 4 -p`** *contraseña* donde *contraseña* es la contraseña de topología. El parámetro **`-threadCount`** especifica el número de hebras utilizadas al copiar los archivos de instalación. Se puede cambiar el valor si es necesario.

   Los archivos necesarios para cada servidor de destino se copian desde servidor de instalación a los servidores de destino. Este paso puede tardar hasta dos horas.

   Se muestran mensajes que indican el progreso de subida. Los mensajes indican el estado del componente subido. El estado será uno de los valores siguientes:

   [OK] Componente subido correctamente.

   [Fail]
   La subida del componente ha fallado.
4. Opcional: Si está instalando en un entorno virtualizado, tome una instantánea de todos los servidores de destino. Apague las máquinas virtuales antes de tomar instantáneas para ahorrar espacio de disco y tiempo de proceso. Después de tomar la instantánea, reinicie las máquinas virtuales. Se puede utilizar la instantánea para reiniciar la instalación desde este punto si se producen errores durante el procesamiento de instalaciones posteriores.
5. Prepárese para la ejecución de la fase 1 de instalación.
   a. Utilizando el editor de texto, edite el archivo de propiedades de topología: *`inicio_instalación`*`/ioc/topology/iop_lite_topo.properties`.
   b. Cambie los valores de estado como se indica:

      ```
      Status.Phase1="New"
      Status.Phase2="Ready"
      ```

      Esto le dirá al programa de instalación que instale la primera fase y salte a la segunda fase.
   c. Cambie al directorio *`inicio_instalación`*`/ioc`.
   d. Ejecute el mandato **`cp topology/iop_lite_topo.template.xml topology/iop_lite_topo.xml`**. El archivo de plantilla topología se copiará en el archivo de topología.

e. Ejecute el mandato **bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p** *contraseña* donde *contraseña* es la contraseña de topología. Los valores de propiedad definidos en el archivo de propiedades de topología se aplicarán al archivo de topología.

f. Opcional: Ejecute el mandato **bin/ba.sh encryptTopology -t iop_lite_topo -p** *contraseña* donde *contraseña* es la contraseña de topología. Las contraseñas del archivo de topología se cifrarán utilizando la contraseña de topología proporcionada.

6. Ejecute la fase 1 de la instalación.
   a. Cambie al directorio *inicio_instalación*/ioc.
   b. Ejecute el mandato **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
   c. Ejecute el mandato **bin/ba.sh installTopology -t iop_lite_topo -p** *contraseña*, donde *contraseña* es la contraseña de la topología.

   La instalación instala los componentes base necesarios para IBM Intelligent Operations Center. Este paso puede tardar hasta 9 horas en ejecutarse.

   Se visualizan mensajes que indican el progreso de la instalación. Los mensajes indican el estado del componente instalado. El estado será uno de los valores siguientes:

   [OK] Componente instalado correctamente.

   [Fail]
   Se ha encontrado un error en la instalación del componente.
7. Opcional: Si está instalando en un entorno virtualizado, tome una instantánea de todos los servidores de destino. No cierre los servidores virtuales antes de tomar la instantánea. Al tomar la instantánea, incluya una instantánea de la memoria de máquina virtual. Se puede utilizar la instantánea para reiniciar la instalación desde este punto si se producen errores durante el procesamiento de instalaciones posteriores.
8. Prepárese para la ejecución de la fase 2 de instalación.
   a. Utilizando el editor de texto, edite el archivo de propiedades de topología: *inicio_instalación*/ioc/topology/iop_lite_topo.properties.
   b. Cambie los valores de estado como se indica:

      ```
      Status.Phase1="Ready"
      Status.Phase2="New"
      ```

      Esto le dirá al programa de instalación que instale la segunda fase y salte a la primera fase.
   c. Cambie al directorio *inicio_instalación*/ioc.
   d. Ejecute el mandato **cp topology/iop_lite_topo.template.xml topology/iop_lite_topo.xml**. El archivo de plantilla topología se copiará en el archivo de topología.
   e. Ejecute el mandato **bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p** *contraseña* donde *contraseña* es la contraseña de topología. Los valores de propiedad definidos en el archivo de propiedades de topología se aplicarán al archivo de topología.
   f. Opcional: Ejecute el mandato **bin/ba.sh encryptTopology -t iop_lite_topo -p** *contraseña* donde *contraseña* es la contraseña de topología. Las contraseñas del archivo de topología se cifrarán utilizando la contraseña de topología proporcionada.
9. Ejecute la fase 2 de la instalación.
   a. Cambie al directorio *inicio_instalación*/ioc.
   b. Ejecute el mandato **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
   c. Ejecute el mandato **bin/ba.sh installTopology -t iop_lite_topo -p** *contraseña*, donde *contraseña* es la contraseña de la topología.

   La instalación instala los componentes restantes necesarios para IBM Intelligent Operations Center. Este paso puede tardar hasta 4 horas en ejecutarse.

Se visualizan mensajes que indican el progreso de la instalación. Los mensajes indican el estado del componente instalado. El estado será uno de los valores siguientes:

[OK] Componente instalado correctamente.

[Fail]
Se ha encontrado un error en la instalación del componente.

Resultados

La arquitectura de IBM Intelligent Operations Center está instalada correctamente cuando todos los mensajes estén completos con un estado `[ OK ]` .

Reinicio de la instalación de arquitectura IBM Intelligent Operations Center durante una instalación paso a paso

Si la instalación de arquitectura falla, se puede reiniciar la instalación.

Acerca de esta tarea

Para reiniciar una instalación que ha fallado, haga lo siguiente.

Procedimiento

1. Edite el archivo de topología para determinar qué componente ha fallado. Esto se indicará mediante `Status="Uncertain"`.
2. Determine y resuelva la causa del error.La instalación debe reunir herramienta se puede utilizar para recopilar los registros de instalación para su revisión.
3. Vuelva a ejecutar el mandato **`installTopology`** . Se volverá a intentar la instalación. Se instalarán todos los componentes con `Status="New"` y`Status="Uncertain"` . Los componentes con `Status="Ready"` se han instalado correctamente y se saltarán.

Qué hacer a continuación

Algunas veces una instalación de componente fallido no se instalará correctamente. En este caso, debe volver a crear el entorno antes de que se ejecute el mandato **`installTopology`** y, después, volver a iniciar la instalación. Para obtener un entorno con virtualización, se pueden utilizar instantáneas del entorno para revertir rápidamente el sistema al estado en el que estaba antes de que se ejecute el mandato **`installTopology`** .

Tareas relacionadas:

"La ejecución de la instalación debe reunir la herramienta" en la página 305
Los archivos de registro se generan mientras se está instalando IBM Intelligent Operations Center . Hay una herramienta para recopilar estos archivos de registro para su análisis.

Instalación de Herramienta de control de plataforma

El Herramienta de control de plataforma se utiliza para gestionar el entorno de servidor de IBM Intelligent Operations Center . La herramienta se instalada independiente del producto.

Antes de empezar

El producto IBM Intelligent Operations Center tiene que estar instalado antes de instalar Herramienta de control de plataforma.

Acerca de esta tarea

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Procedimiento

1. En el servidor de instalación, abra una ventana de terminal e inicie sesión como `root`. Si no se inicia sesión como `root`, cambie e la cuenta `root` utilizando el mandato **su -**.
2. Cambie al directorio *install_home*`/isp/mgmt/setup`.
3. Ejecute el mandato **./iopmgmt-install.sh -f** *inicio_instalación*`/ioc/topology/iop_lite_topo.properties` **-p** *contraseña* donde *contraseña* es la contraseña que desea utilizar al acceder a la herramienta. Recuerde esta contraseña porque la necesitará al ejecutar la herramienta. Se ha instalado correctamente Herramienta de control de plataforma en servidor de gestióncuando todos los componentes se muestran instalados con el estado `[ OK ]`.
4. Opcional: Si no utiliza el Java proporcionado por IBM Intelligent Operations Center, en servidor de gestión edite los archivos `/opt/IBM/ISP/mgmt/scripts/CommandEngine.sh` y `/opt/IBM/ISP/mgmt/scripts/UpdateProperty.sh`. Cambie el valor de `export JAVA_HOME=` en los archivos de la ubicación Java JRE del servidor.

Qué hacer a continuación

Verifique que Herramienta de control de plataforma se haya instalado correctamente iniciando, deteniendo y consultando los servicios mediante Herramienta de control de plataforma.

Conceptos relacionados:

"Archivos de topología de instalación" en la página 36
IBM Intelligent Operations Center se ha instalado utilizando un archivo de topología. El archivo de topología es un archivo XML que define los parámetros y los valores utilizados cuando se despliega IBM Intelligent Operations Center en los servidores y define la secuencia utilizada para desplegar los componentes.

Tareas relacionadas:

"Inicio de los servicios" en la página 199
Herramienta de control de plataforma está disponible para iniciar los servicios en ejecución en los servidores IBM Intelligent Operations Center.

"Detención de los servicios" en la página 203
Herramienta de control de plataforma está disponible para detener los servicios de IBM Intelligent Operations Center.

"Consulta del estado de los servicios" en la página 206
Herramienta de control de plataforma está disponible para determinar el estado de los servicios de IBM Intelligent Operations Center.

Instalación de la herramienta Comprobación de verificación del sistema

La herramienta Comprobación de verificación del sistema se utiliza para verificar el estado operativo de los componentes en IBM Intelligent Operations Center. La herramienta se instalada independiente del producto.

Antes de empezar

El producto IBM Intelligent Operations Center tiene que estar instalado antes de instalar la herramienta Comprobación de verificación del sistema .

Acerca de esta tarea

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Procedimiento

1. En el servidor de instalación, abra una ventana de terminal e inicie sesión como `root`. Si no se inicia sesión como `root`, cambie e la cuenta `root` utilizando el mandato **su -**.
2. Ejecute el mandato **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.
3. Cambie al directorio *install_home*`/cat/bin` .
4. Ejecute el mandato **./install-cat-lite.sh -d** *inicio_instalación*`/cat` **-f** *inicio_instalación*`/ioc/topology/iop_lite_topo.properties` **-p** *contraseña* donde *contraseña* es la contraseña de topología.

   Nota: El mandato se tiene que ejecutar desde el directorio *install_home*`/cat/bin` .
   La herramienta Comprobación de verificación del sistema está instalada correctamente cuando se muestran todos los componentes instalados con el estado `[ OK ]` .
5. Reinicie todos los servidores de IBM Intelligent Operations Center.
   a. Cierre todos los servidores de IBM Intelligent Operations Center con elHerramienta de control de plataforma.
   b. Cierre y reinicie todos los servidores desde el sistema operativo.
   c. Inicie todos los servidores de IBM Intelligent Operations Center con el Herramienta de control de plataforma.

Qué hacer a continuación

Verifique que la herramienta Comprobación de verificación del sistema se ha instalado correctamente ejecutando la herramienta Comprobación de verificación del sistema .

Tareas relacionadas:

"Cómo utilizar la herramienta Comprobación de verificación del sistema" en la página 214
La herramienta Comprobación de verificación del sistema se utiliza para determinar el estado operativo de los servicios que forman el sistemaIBM Intelligent Operations Center.

"Detención de los servicios" en la página 203
Herramienta de control de plataforma está disponible para detener los servicios de IBM Intelligent Operations Center.

"Inicio de los servicios" en la página 199
Herramienta de control de plataforma está disponible para iniciar los servicios en ejecución en los servidores IBM Intelligent Operations Center.

Instalación de la aplicación IBM Intelligent Operations Center

Instale la aplicación IBM Intelligent Operations Center después de que la arquitecturaIBM Intelligent Operations Center , incluyendo Comprobación de verificación del sistema y Herramienta de control de plataforma, esté instalada.

Antes de empezar

La arquitectura IBM Intelligent Operations Center tiene que estar instalada y todos los servidores iniciados.

Procedimiento

1. En el servidor de instalación, abra una ventana de terminal e inicie sesión como `root`. Si no se inicia sesión como `root`, cambie e la cuenta `root` utilizando el mandato **su -**.
2. Ejecute el mandato **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre**.

3. Cambie al directorio *inicio_instalación*/ioc.
4. Ejecute el mandato **cp topology/iop_lite_topo.xml topology/iop_lite_topo_phase2.xml** .
5. Ejecute el mandato **bin/ba.sh installTopology -t ioc_lite_topo -p** *password* donde *password* es la contraseña de topología. La instalación instala la aplicación IBM Intelligent Operations Center . Este paso puede tardar hasta una hora.

   Se visualizan mensajes que indican el progreso de la instalación. Los mensajes indican el estado del componente instalado. El estado será uno de los valores siguientes:

   [OK] Componente instalado correctamente.

   [Fail]
   Se ha encontrado un error en la instalación del componente.

Resultados

La aplicación IBM Intelligent Operations Center está instalada correctamente cuando todos los mensajes estén completos con un estado [OK] .

Verificación de la instalación

Después de instalar IBM Intelligent Operations Center, verifique que el producto se ha instalado correctamente.

Procedimiento

Inicie todos los servicios.

1. Inicie todos los servicios de IBM Intelligent Operations Center ejecutando Herramienta de control de plataforma con el parámetro **start all** .
2. Compruebe que todos los servicios se han iniciado correctamente revisando los mensajes mostrados.
3. Ejecute todas las pruebas en la herramienta Comprobación de verificación del sistema .
4. Compruebe que todas las pruebas se han ejecutado correctamente.

Opcionalmente cierre y reinicie todos los servicios.

5. Detenga todos los servicios de IBM Intelligent Operations Center ejecutando Herramienta de control de plataforma con el parámetro **stop all** .
6. Compruebe que todos los servicios se han detenido correctamente revisando los mensajes mostrados.
7. Cierre el sistema operativo Linux en todos los servidores.
8. Apague y encienda todos los servidores de ejecución o vuelva a arrancarlos.
9. Inicie todos los servicios de IBM Intelligent Operations Center ejecutando Herramienta de control de plataforma con el parámetro **start all** .
10. Compruebe que todos los servicios se han iniciado correctamente revisando los mensajes mostrados.
11. Ejecute todas las pruebas en la herramienta Comprobación de verificación del sistema .
12. Compruebe que todas las pruebas se han ejecutado correctamente.

Qué hacer a continuación

Si los errores están anotados, resuélvalos y vuelva a ejecutar estos pasos.

Conceptos relacionados:

"Acerca de" en la página 199
Utilice el portlet Acerca de para ver detalles de la versión del IBM Intelligent Operations Center y el IBM Smarter Cities Software Solutions integrado que ha instalado. También puede ver detalles de las actualizaciones que aplicó desde la instalación.

Tareas relacionadas:

"Inicio de los servicios" en la página 199
Herramienta de control de plataforma está disponible para iniciar los servicios en ejecución en los servidores IBM Intelligent Operations Center.

"Instalación de IBM Intelligent Operations Center utilizando Installation Manager" en la página 26
IBM Intelligent Operations Center puede instalarse utilizando el instalador gráfico proporcionado.

"Detención de los servicios" en la página 203
Herramienta de control de plataforma está disponible para detener los servicios de IBM Intelligent Operations Center.

"Cómo utilizar la herramienta Comprobación de verificación del sistema" en la página 214
La herramienta Comprobación de verificación del sistema se utiliza para determinar el estado operativo de los servicios que forman el sistemaIBM Intelligent Operations Center.

Configuración posterior a la instalación de IBM Intelligent Operations Center

Después de instalar la arquitectura de IBM Intelligent Operations Center utilizando el gestor de instalación o el paso a paso, se tienen que realizar varios pasos de configuración posterior a la instalación para completarla.

Importante: Todo el trabajo de configuración posterior a la instalación debe realizarse antes de que se instale Cyber Hygiene.

Tareas relacionadas:

"Instalación de IBM Intelligent Operations Center utilizando Installation Manager" en la página 26
IBM Intelligent Operations Center puede instalarse utilizando el instalador gráfico proporcionado.

Configuración de servicios de colaboración para IPv6

Si la instalación utiliza redes IPv6, los pasos de configuración son necesarios para los servicios de colaboración.

Acerca de esta tarea

La arquitectura de IBM Intelligent Operations Center tiene que estar instalada antes de la configuración de redes IPv6 para servicios de colaboración.

Procedimiento

1. Siga los pasos de la documentación de Lotus Domino para configurar Lotus Domino para el direccionamiento IPv6.
2. Siga los pasos de la documentación de Lotus Sametime Standard para configurar Lotus Sametime Standard para el direccionamiento IPv6.
3. Siga los pasos de la documentación de WebSphere Portal para configurar la confianza del portlet Lista de contactos de Sametime si no está usando una red IPv4 con una dirección IPv4 asignada a servidor de sucesos .

Información relacionada:

Configuración de Lotus Domino para direccionamiento IPv6

Configuración del servidor de comunidad de Sametime para admitir IPv6

Configuración de la confianza para el portlet Lista de contactos de Sametime

Configuración del inicio de sesión único para servicios de colaboración

Importe la señal de LTPA de SSO WebSphere Portal a servidor de sucesos para permitir que los usuarios acceder a servicios de colaboración sin tener que volver a entrar las credenciales.

Acerca de esta tarea

La arquitectura IBM Intelligent Operations Center tiene que instalarse antes de importar la señal de Lightweight Third-Party Authentication (LTPA).

Esta señal se creó durante la instalación de la arquitectura de IBM Intelligent Operations Center .

Procedimiento

1. Instale un cliente Lotus Notes 8.5.x en la estación de trabajo. Se puede utilizar una instalación existente. La estación de trabajo tiene que poder conectarse aservidor de sucesos a través de TCP/IP utilizando el nombre de host completo.
2. Copie el archivo `/opt/pdweb/etc/stproxy.ltpa` desde servidor de aplicaciones a la estación de trabajo que ejecuta Lotus Notes. Esta es una señal LTPA que se importará al directorio del servicio de colaboración.
3. Copie el archivo `/local/notesdata/admin.id` desde servidor de sucesos a la estación de trabajo ejecutando Lotus Notes. Este es el archivo de ID para el administrador del servicio de colaboración. Utilizará este ID para iniciar sesión en el directorio de los servicios de colaboración.
4. En la estación de trabajo, inicie el cliente Lotus Notes e inicie sesión con el archivo `admin.id` .
   a. En el registro de Lotus Notes en el panel, pulse **Nombre de usuario**.
   b. Vaya al directorio donde copió ese archivo `admin.id` y selecciónelo.
   c. Introduzca la contraseña definida en el archivo de propiedades de topología para la propiedad `DOMINO.ADMIN.PWD`.
   d. Pulse **Sí** si se muestra una advertencia de seguridad.
5. Abra el archivo `names.nsf`.
   a. Haga clic en **Archivo** > **Abrir** > **Aplicación Lotus Notes**.
   b. Entre el nombre de host completo de servidor de sucesos en **Pasar**.
   c. Entre `names.nsf` en **Nombre de archivo**.
   d. Pulse **Abrir**.
6. Navegue a **Web** > **Configuraciones de web**.
7. Seleccione `Configuración web de SSO para señal de LTPA` y pulse **Editar documento**.
8. Haga clic en **Claves** > **Importar claves LTPA de WebSphere**. Pulse **Aceptar** si se recibe una advertencia acerca de la sobrescritura de las claves existentes.
9. Entre la vía de acceso donde se copió el archivo `stproxy.ltpa` . Pulse **Aceptar**.
10. Entre la contraseña para la señal de LTPA. La contraseña se define en la propiedad `WAS.LTPA.PWD` del archivo de propiedades de topología.
11. Pulse **Aceptar** > **Guardar y cerrar**.
12. Reinicie el servicio de configuración utilizando Herramienta de control de plataforma.

a. Inicie sesión en servidor de gestión y abra una ventana de terminal.
b. Ejecute **su -ibmadmin**.
c. Ejecute **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop st** *contraseña* donde *contraseña* es la contraseña de Herramienta de control de plataforma definida cuando se ha instalado Herramienta de control de plataforma.
d. Ejecute **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start st** *contraseña* donde *contraseña* es la contraseña de Herramienta de control de plataforma definida cuando se ha instalado Herramienta de control de plataforma.

Configuración del tiempo de espera de sesión

El tiempo de espera de sesión determina el tiempo que puede permanecer un usuario inactivo antes de que termine la sesión o de que el usuario tenga que iniciar sesión de nuevo. El tiempo de espera de sesión incluye a los administradores que inician sesión a través del servicio del portal.

Acerca de esta tarea

Cuando IBM Intelligent Operations Center está instalado, no se define tiempo de espera. Los usuarios permanecerán registrados hasta que cierren sesión aunque la sesión esté inactiva.

Si su organización tiene políticas de seguridad que requieren que las sesiones se cierren después de un periodo de inactividad, utilice los pasos siguientes para definir el tiempo de espera de sesión para el sistema IBM Intelligent Operations Center .

Procedimiento

1. Utilizando un navegador web, vaya a `http://application_server:9060/ibm/console` donde*application_server* es el nombre de host de servidor de aplicaciones.
2. Inicie sesión como usuario `waswebadmin` con la contraseña definida para `PORTAL.ADMIN.ACCOUNT.PWD` en el archivo de propiedades de topología.
3. Pulse **Servidores** > **Tipo de servidor** > **WebSphere Application Server** > **WebSphere Portal**.
4. Pulse **Configuración de contenedor** > **Gestión de sesiones** > **Configurar tiempo de espera**.
5. Entre el valor de tiempo de espera deseado en minutos.
6. Pulse **Aceptar**.
7. Pulse **Guardar**.
8. Pulse **Servidores** > **Tipo de servidor** > **WebSphere Application Servers** > **STProxyServer1**.
9. Pulse **Configuración de contenedor** > **Gestión de sesiones** > **Configurar tiempo de espera**.
10. Entre el valor de tiempo de espera deseado en minutos.
11. Pulse **Aceptar**.
12. Pulse **Guardar**.
13. Pulse **Servidores** > **Tipo de servidor** > **WebSphere Application Servers** > **CongnosX_GW1**.
14. Pulse **Configuración de contenedor** > **Gestión de sesiones** > **Configurar tiempo de espera**.
15. Entre el valor de tiempo de espera deseado en minutos.
16. Pulse **Aceptar**.
17. Pulse **Guardar**.
18. Pulse **Servidores** > **Tipo de servidor** > **WebSphere Application Servers** > **CongnosX_Disp1**.
19. Pulse **Configuración de contenedor** > **Gestión de sesiones** > **Configurar tiempo de espera**.
20. Entre el valor de tiempo de espera deseado en minutos.
21. Pulse **Aceptar**.
22. Pulse **Guardar**.
23. Detenga y reinicie servidor de aplicaciones

24. En el registro de servidor de aplicaciones inicie sesión como usuario `ibmadmin` con la contraseña definida para `IOP.ADMIN.USER.PWD` en el archivo de propiedades de topología.
25. Ejecute el mandato **`sudo su -`** para intercambiar el usuario `root` .
26. Edite el archivo `/opt/pdweb/etc/webseald-default.conf` con un editor de texto.
27. En la sección`SESSION CACHE SETTINGS` cambie el valor `timeout = 0` al tiempo de espera de sesión deseado en segundos. El tiempo de espera debe ser el mismo que el tiempo configurado para el servicio de portal. Sin embargo, el valor de portal se establece en minutos y el valor de caché de la sesión se especifica en segundos. El valor de tiempo de espera de los valores caché de la sesión debe ser exactamente 60 veces el valor establecido para el servicio de portal. Por ejemplo, si el valor de portal era de 30 (minutos), el valor de tiempo de espera de los valores caché de la sesión debe ser de 1800 (segundos).
28. Ejecute el mandato **`/usr/bin/pdweb restart`** para reiniciar el servicio de seguridad.

Instalación y configuración de servicios de modelo semántico

IBM Intelligent Operations Center proporciona una aplicación de servicios de modelo semántico y un modelo de muestra. Este servicio debe instalarse y configurarse antes de utilizarlo.

Configuración del servidor de equipo Jazz

El IBM Intelligent Operations Center servicios de modelo semántico está instalado en un servidor de equipo Jazz. El servidor de equipo Jazz debe configurarse antes de que se instalen los servicios de modelo semántico de IBM Intelligent Operations Center.

Acerca de esta tarea

La arquitectura de IBM Intelligent Operations Center debe instalarse antes de configurarse el servidor de equipo Jazz.

Procedimiento

1. En un navegador web, vaya a `http://`*`host_gestión`*`:82/jts/setup` donde *host_gestión* es el nombre de host completo del servidor de gestión.
2. Inicie sesión con el ID de usuario `iicsystemuser` y la contraseña `passw0rd`.
3. Pulse **Siguiente**.
4. En la página Configurar URI público, especifique un valor **Raíz de URI público** con el formato `https://`*`host_gestión`*`:9448/jts` y seleccione `Entiendo que una vez que el URI público se ha establecido, no puede modificarse.`. Pulse **Siguiente**.
5. Pulse en **Probar conexión**. Se debe visualizar un mensaje indicando que la prueba de configuración ha sido satisfactoria.
6. Pulse **Siguiente** para guardar los valores y continuar.
7. Configure la base de datos en la página Configurar base de datos.
   a. Seleccione `DB2` para **Proveedor de base de datos**.
   b. Seleccione `JDBC` para **Tipo de conexión**.
   c. Escriba la contraseña de la base de datos DB2 definida como la propiedad `DEFAULT.PWD.DB2` en el archivo de propiedades de topología para **Contraseña JDBC**. Ignore el mensaje de la contraseña que se visualiza.
   d. Para **Ubicación de JDBC**, escriba `//`*`host_base_datos`*`:50005/JTS:user=db2inst5;password={password};` donde *host_base_datos* es el nombre de host del servidor de datos. La serie {password} debe especificarse tal como se muestra. No la sustituya por un valor de contraseña.
   e. Pulse en **Probar conexión**. Si se produce un error, compruebe y corrija las entradas necesarias. Si las entradas son correctas, asegúrese de que los servicios de base de datos se han iniciado en el servidor de datos utilizando la Herramienta de control de plataforma.

f. Después de que se visualice un mensaje indicando que no hay ninguna tabla Jazz en la base de datos, pulse **Crear tablas**. El proceso tardará varios minutos en completarse.
g. Pulse **Siguiente**.

8. En la página Habilitar notificación por correo electrónico, establezca el valor en **Inhabilitado** y pulse **Siguiente.**
9. La página Registrar aplicaciones debería mostrar "No se han detectado aplicaciones nuevas". Pulse **Siguiente**.
10. Seleccione **LDAP** para el **Tipo de registro de usuarios** en el Paso 1 de la página Configurar registro de usuarios.
11. En el Paso 2, configure LDAP para el registro del servidor de equipo Jazz.
    a. Especifique `ldap://host_gestión:389` para **Ubicación de registro LDAP** donde *host_gestión* es el nombre de host completo del servidor de gestión.
    b. Especifique `OU=USERS,OU=SWG,O=IBM,C=US` para **DN de usuario base**.
    c. Especifique `userId=uid,name=cn,emailAddress=mail` para **Correlación de nombres de propiedad de usuario**.
    d. Especifique `OU=GROUPS,OU=SWG,O=IBM,C=US` para **DN de grupo base**.
    e. Para **Correlación de Jazz con grupos LDAP**, asegúrese de que el valor está establecido en `JazzAdmins=JazzAdmins, JazzUsers=JazzUsers, JazzDWAdmins=JazzDWAdmins, JazzProjectAdmins=JazzProjectAdmins, JazzGuests=JazzGuests`.
    f. Especifique `cn` para **Propiedad de nombre de grupo**.
    g. Especifique `cn` para **Propiedad de miembro de grupo**.
12. Pulse en **Probar conexión**. Si se visualiza un mensaje de aviso, pulse **mostrar detalles**. Si el aviso es acerca de la propiedad `mail`, puede ignorar el mensaje.
13. Para **Tipo de licencia de acceso de cliente**, seleccione `IBM Integrated Information Core - IIC Model Server`.
14. Pulse **Siguiente**.
15. Para **Configurar almacén de datos**, marque el recuadro de selección `No deseo configurar el almacén de datos en este momento`.
16. Pulse **Finalizar** en la página Resumen.

Resultados

El servidor de equipo Jazz está operativo.

Instalación de servicios de modelo semántico

El servicios de modelo semántico y la aplicación de ejemplo se proporcionan con IBM Intelligent Operations Center.

Acerca de esta tarea

Se requiere configurar el servidor de equipo Jazz en el servidor de gestión antes de utilizar los servicios de modelo semántico.

Procedimiento

1. En un navegador web, vaya a `http://host_gestión:82/jts/admin` donde*host_gestión* es el nombre de host completo del servidor de gestión.
2. En la página Administración de servidor, pulse **Servidor** > **Configuración** > **Registrar aplicaciones**.
3. Pulse **Añadir** en la página Aplicaciones registradas.
4. Añada la aplicación Servidor de modelos en la página Añadir aplicación.
    a. Escriba `Servidor de modelos` para **Nombre de aplicación**.

b. Escriba `http://host_gestión:82/modelserver/scr`, donde *host_gestión* es el nombre de host completo del servidor de gestión, para el **URL de descubrimiento**.
c. Especifique un valor de su elección para **Secreto de consumidor**. Este valor se utilizará para proporcionar acceso a la aplicación. El valor debe tratarse con la misma seguridad que una contraseña.
d. Especifique `iicsystemuser` para **ID funcional**

El **Tipo de aplicación** cambiará a `Servidor de modelos`.

5. Si no hay errores, pulse **Finalizar**.

Verificación de la configuración de los servicios de modelo semántico

Una aplicación de muestra de los servicios de modelo semántico se proporciona con IBM Intelligent Operations Center y puede utilizarse para verificar la instalación y configuración correctas de los servicios de modelo semántico.

Procedimiento

1. Prepare los archivos de modelo de muestra
   a. En el servidor de instalación, busque el archivo `iic15_2_stagebuildtoserver.xx.jar` en el directorio *soporte_instalación*.
   b. Expanda el archivo `iic15_2_stagebuildtoserver.xx.jar` en un directorio de su elección. En los pasos restantes, este directorio se denomina *inicio_modelo*.
2. Instale el modelo de muestra.
   a. En un navegador web del servidor donde se encuentra *inicio_modelo*, vaya a `http://host_gestión:82/iic/console` donde *host_gestión* es el nombre de host completo del servidor de gestión.
   b. Inicie sesión como usuario `iicsystemuser` con `passw0rd` como contraseña.
   c. Pulse **Administrador de modelos** > **Ontologías** > **Examinar**.
   d. Vaya al directorio *soporte_instalación*`/ioc/image/IIC/install/modelServices/post_install/`.
   e. Abra el archivo `rsm.owl`.
   f. Pulse **Cargar**. El archivo se cargará.
   g. Pulse **Administrador de modelos** > **Ontologías** > **Examinar**.
   h. Vaya al directorio *soporte_instalación*`/ioc/image/IIC/install/modelServices/post_install/`.
   i. Abra el archivo `modelServer.owl`.
   j. Pulse **Cargar**. El archivo se cargará.
   k. Pulse **Administrador de modelos** > **Ontologías** > **Examinar**.
   l. Vaya al directorio *soporte_instalación*`/ioc/image/IIC/install/ktpRuntimeServices/post_install/`.
   m. Abra el archivo `kpi.owl`.
   n. Pulse **Cargar**. El archivo se cargará.
   o. Pulse **Administrador de modelos** > **Cargar** > **Examinar**
   p. Vaya al directorio *soporte_instalación*`/ioc/image/IIC/samples/rdf/rsm/`.
   q. Abra el archivo `IBMOilDownstreamSampleRDF.xml`.
   r. Pulse **Cargar**. El archivo se cargará.
   s. Pulse **Administrador de modelos** > **Cargar** > **Examinar**
   t. Vaya al directorio *soporte_instalación*`/ioc/image/IIC/samples/rdf/rsm/`.
   u. Abra el archivo `IBMOilUpstreamSampleRDF.xml`.
   v. Pulse **Cargar**. El archivo se cargará.
   w. Pulse **Administrador de modelos** > **Cargar** > **Examinar**
   x. Vaya al directorio *soporte_instalación*`/ioc/image/IIC/samples/rdf/rsm/`.

y. Abra el archivo `IBMOilDownstreamSampleReferenceRDF.xml`.
z. Pulse **Cargar**. El archivo se cargará.
aa. Pulse **Administrador de modelos** > **Cargar** > **Examinar**
ab. Vaya al directorio *soporte_instalación*`/ioc/image/IIC/samples/rdf/rsm/`.
ac. Abra el archivo `IBMOilUpstreamSampleReferenceRDF.xml`.
ad. Pulse **Cargar**. El archivo se cargará.

3. Verifique que el modelo de muestra está instalado correctamente.
   a. Pulse **Administrador de modelos** > **Consultar** > **Consultar**. Se ejecutará una consulta predefinida. Se visualizará una estructura XML con los resultados de la consulta. La etiqueta de nivel superior debe ser `spargl` y debe tener las etiquetas secundarias `head` y `results`.
   b. Pulse **Explorador de modelos** y asegúrese de que puede examinar el modelo.
4. Utilice el modelo para verificar la instalación del administrador de modelos.
   a. En un navegador web en el servidor de gestión, vaya a `http://`*`host_gestión`*`:82/iic/ibmoil` donde *host_gestión* es el nombre de host completo del servidor de gestión.
   b. Pulse **IBM Oil Company** > **Variables**. Se visualizan los URL de servicios web.

Resultados

Los servicios de modelo semántico y el modelo de muestra IBMOil se instalarán.

Mejora del rendimiento de servicios de modelo semántico

Configure el servicios de modelo semántico proporcionado porIBM Intelligent Operations Center para mejorar el rendimiento al ejecutar consultas en modelos.

Procedimiento

1. En un navegador web, vaya a `http://`*`host_gestión`*`:82/iic/console` donde*host_gestión* es el nombre de host completo del servidor de gestión.
2. Añada los valores de propiedad de la Tabla 20 a la categoría **OPCWEBSERVICE**.

Tabla 20. Propiedades de OPCWEBSERVICE

Propiedad	Valor
`cache.browse.timetolive.second`	3600
`cache.timetolive.second`	2592000
`cache.wait.second.after.create.action`	1

3. Actualice o añada las siguientes propiedades y valores de la Tabla 21 en la página 60 en la categoría RSM.

Tabla 21. Propiedades de RSM

Propiedad	Valor
mvmViewPath.0	http://iec.ch/TC57/CIMgeneric# ISA95_Enterprise##http://iec.ch/TC57/ CIMgeneric# RSM_OrganizationalEntity.ManagesAspectOf_PhysicalEntity ##iec.ch/TC57/CIMgeneric# ISA95_Site##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_Area##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_ProductionUnit##http:// iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.ManagedBy_OrganizationalEntity##http:// iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity##http:// iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.has_measurement##http:// iec.ch/TC57/CIM-generic#RSM_Measurement##http:// iec.ch/TC57/ CIMgeneric# RSM_Measurement.HasA_MeasurementValue##http:// iec.ch/TC57/CIM-generic#RSM_MeasurementValue
mvmViewPath.1	http://iec.ch/TC57/CIMgeneric# ISA95_Enterprise##http://iec.ch/TC57/ CIMgeneric# RSM_OrganizationalEntity.ManagesAspectOf_PhysicalEntity ##iec.ch/TC57/CIMgeneric# ISA95_Area##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_ProductionUnit##http://iec.ch/TC57/CIMgeneric# ISA95_WorkCenter.Contains_Equipment##http:// iec.ch/TC57/CIMgeneric# RSM_WorkEquipment##http:// iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.has_measurement##http:// iec.ch/TC57/CIM-generic#RSM_Measurement##http:// iec.ch/TC57/CIMgeneric# RSM_Measurement.HasA_MeasurementValue##http:// iec.ch/TC57/CIM-generic#RSM_MeasurementValue
mvmDownLevelPreRequest	3
mvmCacheProperty.0	cim:RSM_IdentifiedObject.name
mvmMaxQueryURI	500
mvmMaxSparqlEntry	4000

4. Pulse **Publicar**. Se guardarán las propiedades nuevas y modificadas.
5. Reinicie los servicios de modelo semántico utilizando la Herramienta de control de plataforma.
6. En un navegador web, vaya a `http://`*`host_gestión`*`:82/iic/console` donde*host_gestión* es el nombre de host completo del servidor de gestión.
7. Aplique los cambios específicos de solución o aplicación según convenga. Si los cambios son necesarios, se identificarán en la documentación del producto o de la solución.

Configuración del Herramienta de control de plataforma

Después de instalar IBM Intelligent Operations Center, si ha instalado un JRE de Java diferente del proporcionado con IBM Intelligent Operations Center tiene que definir la ubicación de JRE utilizado por Herramienta de control de plataforma.

Procedimiento

1. En servidor de gestión, edite el archivo `/opt/IBM/ISP/mgmt/scripts/CommandEngine.sh` .
2. Cambie `export JAVA_HOME=` a la ubicación del JRE Java .
3. Guarde los cambios.
4. En servidor de gestión, edite el archivo `/opt/IBM/ISP/mgmt/scripts/UpdateProperty.sh` .
5. Cambie `export JAVA_HOME=` a la ubicación del JRE Java .
6. Guarde los cambios.

Tareas relacionadas:

"Instalación del entorno de tiempo de ejecución Java" en la página 26
El entorno de ejecución Java 6 debe estar instalado en servidor de instalación antes de instalar IBM Intelligent Operations Center.

Cifrado de la contraseña administrativa de Tivoli Service Request Manager

Utilice el siguiente procedimiento para cifrar la contraseña administrativa deTivoli Service Request Manager en Tivoli Netcool/Impact.

Procedimiento

1. Inicie sesión en la consola de administración de Tivoli Netcool/Impact `http://host_suceso:9080/nci/main` donde *host_suceso* es el nombre de host de servidor de sucesos.Inicie sesión como usuario `admin` con la contraseña `netcool`.
2. Pulse **Proyectos de IOC** .
3. En la sección Políticas, haga doble clic en la política **IOC_Sample_Password_Encoder**. Se abre la política en la ventana Editor de políticas .
4. En el campo **Entre aquí contraseña** , entre la contraseña para `Maxadmin`. La contraseña `Maxadmin` es la contraseña de usuario administrativo especificada durante la instalación.
5. Para guardar la política, pulse **Guardar**.
6. Pulse el icono **Política de desencadenador** .
7. Haga clic en **Ejecutar**.
8. En la sección Estados del servicio, desplácese hasta **PolicyLogger**, pulse **Ver registro de PolicyLogger** (icono con la flecha hacia abajo).
9. En la ventana del registrador de políticas, busque la sentencia parecida a la siguiente:
   ```
   11 May 2012 14:19:12,260: [IOC_Sample_Password_Encoder][pool-1-thread-46]Parser log: {aes}FF877B74ADF4DF1C2002F94ACB38FAFF
   ```
10. Copie la contraseña**Maxadmin** cifrada de la sentencia, por ejemplo:
    ```
    {aes}FF877B74ADF4DF1C2002F94ACB38FAFF
    ```
11. En la consola administrativa Tivoli Netcool/Impact , en la sección Políticas, haga doble clic en la política **UTILS_LIBRARY_IOC_TSRM**. Se abre la política en la ventana Editor de políticas .
12. Sustituya el valor de *MAXAdminPassword* por el valor cifrado que copió en el paso 10:
    ```
    MAXAdminPassword = "{aes}FF877B74ADF4DF1C2002F94ACB38FAFF";
    ```
13. Para guardar la política, pulse **Guardar**.
14. Pulse **Proyectos de IOC** .
15. En la sección Políticas, haga doble clic en la política **IOC_Sample_Password_Encoder**. Se abre la política en la ventana Editor de políticas .
16. En el campo **Introduzca aquí la contraseña**, suprima la contraseña de **Maxadmin**.
17. Para guardar la política, pulse **Guardar**.

Establecimiento del número mínimo de hebras de EventProcessor

El número mínimo de hebras de EventProcessor se debe establecer el 25 por motivos de rendimiento.

Procedimiento

1. Inicie sesión en la consola de administración de Tivoli Netcool/Impact `http://host_suceso:9080/nci/main` donde *host_suceso* es el nombre de host de servidor de sucesos.
2. Pulse **Estado del servicio** > **EventProcessor**.
3. Especifique 25 en **Número mínimo de hebras**.

   Nota: El valor **Número mínimo de hebras** no puede superar el valor de **Número máximo de hebras**.

4. Pulse **Aceptar**.
5. Pulse el icono Detener proceso para detener EventProcessor.
6. Pulse el icono Iniciar proceso para iniciar EventProcessor.

Cambio de tamaño de la agrupación de hebras predeterminada y del contenedor web

Es necesario cambiar el tamaño de la agrupación de hebras `predeterminada` y del `contenedor web` para mejorar el rendimiento de los procedimientos operativos estándar.

Procedimiento

1. En servidor de sucesos de la interfaz de administración de WebSphere Portal, pulse **Intelligent Operations** > **Herramientas administrativas** > **Consolas de administración**.
2. En Servidor de sucesos, pulse **Servidor de aplicaciones de procedimiento operativo estándar**.
3. Inicie sesión como administrador de WebSphere Application Server. El ID de usuario se define en la propiedad `WAS.ADMIN.ACCOUNT` y la contraseña se define en la propiedad `WAS.ADMIN.ACCOUNT.PWD` del archivo de propiedades de topología al instalar IBM Intelligent Operations Center.
4. Pulse **Servidores** > **Servidores de aplicación** > **MXServer1** > **Agrupaciones de hebras** > **Contenedor web**.
5. Introduzca `50` para **Tamaño mínimo**.
6. Introduzca `50` para **Tamaño máximo**.
7. Pulse **Aceptar**.
8. Pulse **Servidores** > **Servidores de aplicación** > **MXServer1** > **Agrupación de hebras** > **Predeterminado**.
9. Introduzca `20` para **Tamaño mínimo**.
10. Introduzca `50` para **Tamaño máximo**.
11. Pulse **Aceptar**.
12. Reinicie `TSRMCluster`.
    a. Seleccione **Servidores** > **Clústeres**.
    b. Seleccione `TSRMCluster`.
    c. Pulse **Detener**.
    d. Espere a que el estado cambie a rojo.
    e. Pulse **Iniciar**.

Instalación y ejecución paso a paso de Cyber Hygiene

Cyber Hygiene se ha instalado y ejecutado por separado de IBM Intelligent Operations Center y se debe instalar y ejecutar cuando todos los componentes de IBM Intelligent Operations Center estén instalados, configurados y en funcionamiento. Cyber Hygiene cambia la configuración predeterminada del sistema operativo a un conjunto de opciones más seguras para proteger el sistema IBM Intelligent Operations Center.

Antes de empezar

Nota: Cyber Hygiene está instalado y se ejecuta en el mismo paso. Si está instalando IBM Intelligent Operations Center utilizando IBM Installation Manager, no siga estos pasos. La instalación de IBM Installation Manager proporciona una opción para instalar y ejecutar Cyber Hygiene.

Para reducir el tiempo que Cyber Hygiene invierte en el análisis y la remediación, desmonte el sistema de archivos que no se necesita para la seguridad. Por ejemplo, los directorios *install_media*de cada uno de los

servidores se pueden suprimir después de que se completen todos los pasos de la instalación. Estos directorios se pueden suprimir o desmontar antes de ejecutar Cyber Hygiene.

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Acerca de esta tarea

Cyber Hygiene debe ser el último paso después de la instalación de IBM Intelligent Operations Center. El análisis y las remediaciones abordan las exposiciones de seguridad de configuración que existen después de haber instalado el sistema operativo predeterminado y el producto IBM Intelligent Operations Center. Las remediaciones aplicadas se han probado para confirmar que los servicios de IBM Intelligent Operations Center funcionarán correctamente.

Los cambios aplicados al sistema por Cyber Hygiene pueden causar problemas con otras aplicaciones y soluciones. Por ejemplo, es posible que otras aplicaciones y soluciones tengan requisitos sobre el entorno Linux que no están de acuerdo con las buenas prácticas de seguridad. Una aplicación o solución puede requerir que el sistema esté iniciado como usuario `root` para instalarse o ejecutarse. En este caso, es posible que algunos de los cambios de Cyber Hygiene sean temporales o permanentes u otra solución encontrada por el proveedor de la aplicación o solución.

Después de haber aplicado los cambios de Cyber Hygiene, no hay ningún método automatizado para cambiarlos. Todos los cambios deben realizarse por medio de actualizaciones manuales al sistema operativo Linux o cambiando los permisos del directorio o archivo.

Procedimiento

1. En el servidor de instalación, abra una ventana de terminal e inicie sesión como `root`. Si no se inicia sesión como `root`, cambie e la cuenta `root` utilizando el mandato **`su -`**.
2. Ejecute el mandato **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`**. La variable `JAVA_HOME` se establece en el entorno de tiempo de ejecución de Java (JRE).
3. Cambie al directorio *`install_home`*`/ch/install` .
4. Edite el archivo `iop-ch-install.xml` utilizando un editor de texto.
5. Sustituya los parámetros del archivo `iop-ch-install.xml` por los valores adecuados para su instalación.

Tabla 22. Parámetros de instalación de Cyber Hygiene

Parámetro	Valor
`${APP.1.HOST}`	Nombre de host completo de servidor de aplicaciones
`${APP.1.ACCT}`	El nombre de usuario de Linux para el acceso SSH a servidor de aplicaciones
`${APP.1.ACCT.PWD}`	Contraseña para `${APP.1.ACCT}`
`${APP.1.SSH_PORT}`	Puerto SSH de servidor de aplicaciones
`${DB.1.HOST}`	Nombre de host completo de servidor de datos
`${DB.1.ACCT}`	El nombre de usuario de Linux para el acceso SSH a servidor de datos
`${DB.1.ACCT.PWD}`	Contraseña para `${DB.1.ACCT}`
`${DB.1.SSH_PORT}`	Puerto SSH de servidor de datos
`${EVENT.1.HOST}`	Nombre de host completo de servidor de sucesos
`${EVENT.1.ACCT}`	El nombre de usuario de Linux para el acceso SSH a servidor de sucesos
`${EVENT.1.ACCT.PWD}`	Contraseña para `${EVENT.1.ACCT}`

Tabla 22. Parámetros de instalación de Cyber Hygiene (continuación)

Parámetro	Valor
${EVENT.1.SSH_PORT}	Puerto SSH de servidor de sucesos
${MGMT.1.HOST}	Nombre de host completo de servidor de gestión
${MGMT.1.ACCT}	El nombre de usuario de Linux para el acceso SSH a servidor de gestión
${MGMT.1.ACCT.PWD}	Contraseña para ${MGMT.1.ACCT}
${MGMT.1.SSH_PORT}	Puerto SSH de servidor de gestión

6. Guarde el archivo.
7. Cambie al directorio *install_home*/ch .
8. Ejecute el mandato *inicio_instalación***/ch/install/iop-ch-install.sh -r iop-ch-install-messages.properties -f 'com.ibm.iop.cyber.hygiene.scripts.lite_1.5.0.zip' -d** *soporte_instalación***/ioc/image -p** *contraseña_GRUB* donde *contraseña_GRUB* es la contraseña del cargador de inicio de GRUB en los servidores. Se aplicará *GRUB_password* a todos los servidores de destino. Normalmente, cuando se reinician los servidores, no se necesita contraseña. Sin embargo, una vez que Cyber Hygiene está instalado, si inicia un servidor con cualquier opción de Linux, como el inicio en modalidad de un usuario único, se tendrá que entrar *GRUB_password* en la consola del servidor.

Resultados

El tiempo de proceso se determina por la velocidad del hardware y si hay archivos extra no necesarios en los servidores de destino. El proceso puede llevar hasta 1,5 horas. Durante ese tiempo, se analizarán los servidores de destino y se aplicará la remediación adecuada.

Qué hacer a continuación

Compruebe el registro de Cyber Hygiene para ver cualquier error. Los registros mostrarán las remediaciones aplicadas y los pasos manuales opcionales.

Conceptos relacionados:

"Descripción general de Cyber Hygiene" en la página 84
La función Cyber Hygiene de IBM Intelligent Operations Center está diseñada para proporcionar servicios que solucionen exposiciones de seguridad potenciales en el sistema instalado.

Cambios en el sistema operativo Linux

Cyber Hygiene busca en el sistema operativo Linux exposiciones de seguridad conocidas y realiza los cambios apropiados. Los registros describen las exposiciones exploradas y los cambios realizados en las políticas y en la configuración del SO Linux.

Los registros también listan las exposiciones que se han detectado, pero en las que no se han realizado cambios. Estos pueden incluyen:

- El sistema ya está configurado tal como Cyber Hygiene lo habría cambiado.
- El cambio requiere que el administrador del sistema tome medidas o decida si el cambio es adecuado al entorno.
- El cambio no se puede realizar por medio de un script automatizado. Por ejemplo, la exposición está relacionada con las políticas de seguridad generales de la empresa.

Las remediaciones aplicadas por Cyber Hygiene se pueden cambiar más adelante si es necesario. Los registros de Cyber Hygiene proporcionan información sobre los cambios aplicados en el sistema. Es posible que los cambios requieran el uso del sistema con otras aplicaciones o soluciones si los cambios realizados por Cyber Hygiene son incompatibles con los sistemas en cuestión.

Revisión del registro de Cyber Hygiene

Cuando Cyber Hygiene esté instalado y en ejecución, revise el registro para comprender los cambios realizados en el sistema y las exposiciones restantes.

Acerca de esta tarea

En el servidor de instalación, vaya al directorio en el que se ha copiado el paquete de instalación de IBM Intelligent Operations Center. En estos pasos, este directorio se conoce como *inicio_instalación*.

Procedimiento

1. Revise el registro de Cyber Hygiene en el directorio `/var/ibm/InstallationManager/logs/native` de servidor de instalación para asegurarse de que se hayan realizado todas las acciones en todos los servidores. El registro se puede encontrar ejecutando el mandato **`fgrep yber *.log`**. El archivo de registro mostrará información para cada servidor. En general, los pasos con la información de registro incluyen:
   - Preparación del entorno para ejecutar las tareas de Cyber Hygiene.
   - Ejecución del remediador autónomo. Arregla las exposiciones que no requieren análisis. Por ejemplo, establecimiento de una contraseña del gestor de arranque GRUB y activación de la auditoría.
   - Inhabilitación del inicio de sesión root remoto.
   - Análisis de exposiciones. Se están ejecutando en un segundo plano y las tareas principales esperan a que se complete el análisis.
   - Ejecución del remediador para abordar las exposiciones encontradas durante el análisis.
   - Análisis después de la remediación. Identifica las exposiciones que no se han encontrado durante el análisis inicial.
   - Ejecución del remediador para abordar exposiciones adicionales encontradas durante el segundo análisis. Se registran las remediaciones no completadas.
2. Revise los registros detallados de Cyber Hygiene ubicados en el directorio `/var/BA15/CH/results` de cada uno de los servidores de destino. El `standrem-`*`date_time`*`.log` muestra los resultados del remediador autónomo. El `standrem-disableRemoteRoot-`*`date_time`*`.log` muestra los resultados de inhabilitar el inicio de sesión root remoto. El `scanrem-combined-log-`*`date_time`*`.log` muestra los resultados de las acciones de remediador analizadas. Hay dos registros para los dos pasos de análisis/remediación.
   a. Revise los archivos de registro para buscar líneas que empiecen con el texto `Vulnerability`. Cada una de las líneas indica la medida adoptada e incluye:
      - Los hallazgos del análisis.
      - Las remediaciones seleccionadas.
      - Los detalles de las remediaciones aplicadas.
   b. En el registro para el segundo análisis y remediación, las anotadas con el texto `NOT DONE` puede que se tengan que investigar por otras acciones manuales.

Rehabilitación del inicio de sesión de raíz remoto

Cyber Hygiene inhabilita el inicio de sesión remoto en la cuenta `root` a través del mandato **`ssh`**. Los mandatos **`telnet`** y **`rsh`** están completamente inhabilitados en el sistema operativo Linux. Si es necesario, el inicio de sesión remoto se puede volver a habilitar.

Acerca de esta tarea

Es posible que no se necesite volver a habilitar el inicio de sesión remoto para el usuario `root` . Un usuario con privilegios adecuados puede utilizar los mandatos **su** y **sudo** para operar como usuario `root` . Los usuarios privilegiados que funcionan como usuarios `root` están registrados con propósito de auditoría.

IBM Intelligent Operations Centerdefine el usuario `ibmadmin` en el grupo wheel. Los usuarios de este grupo pueden utilizar el mandato **sudo su -** para ejecutarse como `root`.

Procedimiento

Haga lo siguiente para habilitar el inicio de sesión root utilizando el mandato **ssh** .

1. Edite el archivo `/etc/ssh/sshd_config` en el servidor donde es necesario el inicio de sesión remoto como `root` utilizando ssh o una terminal remota.
2. Cambie el parámetro `PermitRootLogin` a `yes` y guarde el archivo. Cambie este parámetro a `no` si el inicio de sesión remoto que utiliza el mandato **ssh** tiene que inhabilitarse.
3. Guarde el archivo.
4. Reinicie el servidor SSH ejecutando el mandato **service sshd restart**.

Cyber Hygiene ha inhabilitado el inicio de sesión remoto en la cuenta `root` mediante terminales remotas. Únicamente el teclado y la pantalla conectados al servidor puede iniciar sesión como usuario `root` . Haga lo siguiente para volver a habilitar el inicio `root` remoto en un servidor desde un terminal remoto.

5. Edite el archivo `/etc/securetty_config` en el servidor donde es necesario el inicio de sesión remoto como `root` utilizando ssh o una terminal remota.
6. Añada nombres de dispositivo Linux para los terminales autorizados para iniciar sesión remotamente como usuario `root` . Por ejemplo, si desea añadir `ttyl`, cambie la lista a leer:

   ```
   consola
   tty1
   ```

   Para inhabilitar un terminal, coloque un carácter # antes del terminal que se va a inhabilitar. Por ejemplo:

   ```
   consola
   #tty1
   ```

7. Guarde el archivo.

Configuración de usuarios que requieren acceso SSH

IBM Intelligent Operations Center requiere que determinados usuarios se configuren con acceso SSH y contraseñas.

Acerca de esta tarea

Los siguientes usuarios se deben configurar en servidor de instalación y en todos los servidores de destino con acceso SSH y contraseñas.

- ibmadmin
- ibmuser
- mqconn

Instalación de herramientas proporcionadas con la solución

Los kits de herramientas y las herramienta de desarrollo se incluyen con IBM Intelligent Operations Center. Se utilizan al personalizar IBM Intelligent Operations Center.

Con la excepción de Rational Application Developer, se proporcionan en la imagen o DVD del kit de herramientas de desarrolladores de IBM Intelligent Operations Center . Rational Application Developer se incluye con IBM Intelligent Operations Center en imágenes o DVD aparte.

Lotus Sametime Client

Para obtener información sobre la instalación y el uso de Lotus Sametime Client , consulte Lotus Domino y el Information Center deLotus Notes .

Kit de herramientas WebSphere Message Broker

Para obtener más información sobre la instalación y el uso del kit de herramientas de WebSphere Message Broker , consulte el Information Center de WebSphere Message Broker .

Kit de herramienta de desarrolladores de IBM WebSphere Business Monitor

Para obtener información sobre la instalación y el uso del kit de herramientas de desarrolladores de IBM WebSphere Business Monitor , consulte el Information Center deIBM WebSphere Business Monitor .

Rational Application Developer

Para obtener información sobre la instalación y uso de Rational Application Developer, consulte el Information Center de Rational Application Developer .

Conceptos relacionados:

"Creación e integración de KPI" en la página 113
Los modelos de KPI se pueden crear y modificar utilizando un kit de herramientas de desarrollo de supervisión de negocio y un portlet de gestión de KPI.

Información relacionada:

Information Center de Lotus Domino y Lotus Notes

Information Center de WebSphere Message Broker

Information Center de IBM Business Monitor

Information Center de Rational Application Developer

Supresión de los usuarios de la muestra

El IBM Intelligent Operations Center se envía con usuarios de muestra. Por motivos de seguridad estos usuarios se deben suprimir cuando se haya instalado IBM Intelligent Operations Center en un entorno de producción.

Acerca de esta tarea

Para suprimir usuarios predefinidos, complete los pasos siguientes:

Procedimiento

1. En servidor de aplicaciones, inicie sesión en WebSphere Portal.
2. En el portal **Administración** , pulse **Acceso** > **Usuarios y grupos** > **Todos los usuarios de portal autenticados**.
3. Pulse en el icono suprimir para los siguientes usuarios:
   - tdelorne
   - scollins

- akelly

Importante: No suprima los siguientes usuarios necesarios. Si usted los elimina, IBM Intelligent Operations Center no funcionará correctamente.

- admin
- iicsystemuser
- maxadmin
- maxintadm
- maxreg
- notesadmin
- resAdmin1
- resDeployer1
- resMonitor1
- rtsAdmin
- rtsConfig
- rtsUser
- taiuser
- SRMSELFSERVICEUSR
- wasadmin
- waswebadmin
- wpsadmin
- wpsbind
- Todos los ID de usuario empiezan por "PM"

Referencia relacionada:

"Usuarios de muestra" en la página 73
Durante el despliegue de IBM Intelligent Operations Center, se crean usuarios de muestra.

Eliminación de los servicios de instalación desde el sistema de producción

Tras instalar IBM Intelligent Operations Center, los servicios de instalación se pueden eliminar de los servidores del sistema de producción. Se recomienda conservar servidor de instalación ya que algunos de sus servicios podrían ser necesarios en actividades de mantenimiento.

Una vez se ha completado la instalación y se ha verificado, los componentes que únicamente se utilizan en el proceso de instalación se pueden eliminar de los servidores del sistema de producción (servidor de aplicaciones, servidor de sucesos, servidor de gestión, servidor de datos). Estos incluyen:

- El directorio definido por la propiedad `Unix.image.basedir.remote` en el archivo de propiedades de topología.
- El directorio definido por la propiedad `Unix.script.basedir.remote` en el archivo de propiedades de topología.
- El directorio *install_media* definido por la propiedad `image.basedir.local` en el archivo de propiedades de topología.

Nota: servidor de instalación debe conservarse en caso de ser necesario en el futuro. Puesto que el archivo de propiedades de topología contiene contraseñas en texto simple, este servidor debe estar en una ubicación segura.

Tareas relacionadas:

"Instalación de IBM Intelligent Operations Center utilizando Installation Manager" en la página 26
IBM Intelligent Operations Center puede instalarse utilizando el instalador gráfico proporcionado.

Capítulo 3. Asegurar la solución

La seguridad es importante dentro de IBM Intelligent Operations Center porque la solución es central para las operaciones esenciales. Para garantizar la seguridad, es importante que sea consciente de la configuración predeterminada y de que gestiona usuarios de la solución para proporcionar a todos los usuarios el nivel de acceso correcto.

Contraseñas predeterminadas

La primera tarea que se debe realizar para proteger la solución es asegurarse de cambiar todas las contraseñas predeterminadas. Para obtener más información sobre las contraseñas predeterminadas, consulte el enlace al final del tema.

Conexión segura

IBM Intelligent Operations Center es compatible con HTTPS de forma predeterminada. Puede cambiar la configuración de HTTPS de los siguientes servicios individuales dentro de IBM Intelligent Operations Center:

- EL servicio de supervisión empresarial que procesa KPI
- El servicio de administración de procedimientos operativos estándar y de recurso

Los cambios realizados en la configuración de HTTPS para un servicio individual se deben acompañar por una actualización en la configuración de puerto correspondiente. Para obtener más detalles sobre cómo cambiar esta configuración en tabla de propiedades del sistema, consulte el enlace al final de este tema

Autenticación de usuario

La autenticación de usuario está asociada con los derechos de autorización que le dan al usuario acceso a las características y datos apropiados. El IBM Intelligent Operations Center admite la integración a la infraestructura de seguridad existentes para un inicio de sesión único.

Los permisos de usuario de IBM Intelligent Operations Center se gestionan a través de grupos y usuarios de WebSphere Portal . WebSphere Portal utiliza la base de datos de Lightweight Directory Access Protocol (LDAP) proporcionada por Tivoli Directory Server que se ejecuta enservidor de datos.

El sistema de seguridad proporcionado conIBM Intelligent Operations Center puede alojar muchos grupos de usuarios, roles y permisos. El alojamiento de muchos grupos de usuarios, roles y permisos puede llevar a un régimen de seguridad que es difícil de gestionar. Se recomienda que los administradores restrinjan el número de grupos y permisos.

Roles de usuario y permisos

La pertenencia de grupo de usuarios basado en roles proporciona una forma de controlar el acceso a IBM Intelligent Operations Center. Los usuarios de un grupo tienen acceso únicamente a las características de la solución que corresponde a su rol. Ser miembro de un grupo de usuarios basado en roles también ayuda a los usuarios a centrarse en las tareas adecuadas. Los roles estándar son: Ejecutivo, Supervisor y Operador.

Para añadir un usuario aIBM Intelligent Operations Center:

1. Elija un grupo adecuado para el rol de usuario de la organización y haga al usuario miembro de ese grupo.

2. Complete un perfil para el usuario e incluya al menos el ID de usuario, el nombre y la contraseña.

Categorías de datos y permisos

La seguridad de datos almacenados en una base de datos de IBM Intelligent Operations Center se gestiona implementando el acceso basado en roles a la base de datos. El acceso a una función de IBM Intelligent Operations Center no significa que todos los datos estén disponibles para el usuario. La seguridad de datos se aplica al nivel de servidor para garantizar que los usuarios vean únicamente los datos apropiados. Las categorías estándar son: Geofísica, Transporte, Meteorología, Medio ambiente, Infraestructura, Química, Biología, Seguridad, Rescate, Fuego, Salud y Otros.

Portal

El servicio de portal proporciona una plataforma que se puede escalar para adaptarse al conjunto necesario de usuarios. También proporciona acceso basado en roles que se puede ajustar para reflejar la estructura de organización requerida. Puede ver, crear y suprimir usuarios o grupos de usuarios con el portlet **Gestionar usuarios y grupos** . También se pueden cambiar los miembros de un grupo. Para obtener más información sobre este portlet, consulte el enlace al final de este tema.

Conceptos relacionados:

"Información de contraseña" en la página 39
Las contraseñas para varios ID de usuario utilizadas en la solución IBM Intelligent Operations Center se definen en el archivo de propiedades de topología. Por razones de seguridad, se deben cambiar las contraseñas predeterminadas que vienen con IBM Intelligent Operations Center .

Información relacionada:

Documentación del producto IBM WebSphere Portal 7

Acceso y roles de usuario

El IBM Intelligent Operations Center implementa la seguridad limitando el acceso a las categorías basadas en roles de usuario.

Para utilizar una característica específica de IBM Intelligent Operations Center, un usuario debe ser miembro del grupo de roles de usuario que proporciona el acceso necesario a esa característica. A un usuario le hace miembro de un grupo de roles de usuario el administrador. La tabla siguiente muestra cómo los roles de la vida real se pueden asignar a los grupos de roles de usuario con niveles de acceso de inicio de sesión en IBM Intelligent Operations Center.

Tabla 23. Roles de trabajo y grupos de roles de usuario de IBM Intelligent Operations Center

Rol del trabajo	Responsabilidades	Grupo de roles de usuario
Director	• Define los umbrales y requisitos de la entrada de sucesos, incidencias e indicadores clave de rendimiento (KPI) • Visualiza resúmenes visuales de alto nivel, detalles e informes de: – KPI – Sucesos • Comunica la política, dirección a largo plazo y decisiones de alto nivel	Ejecutivo en toda la ciudad

Tabla 23. Roles de trabajo y grupos de roles de usuario de IBM Intelligent Operations Center (continuación)

Rol del trabajo	Responsabilidades	Grupo de roles de usuario
Supervisor o gerente	• Gestiona sucesos e incidencias • Produce y supervisa informes de KPI • Emite alertas • Analiza sucesos para requisitos de cambio de estado o acción • Decide sobre medidas correctivas a corto plazo	Supervisor en toda la ciudad
Operador	• Supervisa información del suceso • Supervisa alertas • Visualiza detalles • Emite comunicaciones • Actualiza los datos del suceso o incidencia con más información, por ejemplo: – Informes telefónicos – Entradas para construcciones o mantenimiento	Operador en toda la ciudad
Administrador de usuarios	Administra todos los aspectos de los usuarios incluyendo la definición de grupos, asignación de permisos a grupos y la asignación de usuarios a grupos. Proporciona a los usuarios el nivel de acceso correcto. El nivel de acceso se asigna en base a la pertenencia a grupos.	wpsadmins

Antes de personalizar roles y de definir usuarios para la organización, familiarícese con el sistema de seguridad de IBM Intelligent Operations Center .

Tareas relacionadas:

"Adición de un nuevo usuario o grupo" en la página 78
Seleccione un grupo y crear un perfil de usuario para agregar un nuevo usuario a IBM Intelligent Operations Center . Seleccione un nombre de grupo para agregar un nuevo grupo.

Referencia relacionada:

"Grupos de rol de usuario y permisos de autorización" en la página 74
El conjunto de permisos para acceder a las funciones en IBM Intelligent Operations Center está asociado con cada grupo de rol de usuario.

"Grupos de categorías de usuarios y permisos de datos" en la página 77
El permiso para acceder a una categoría de datos en IBM Intelligent Operations Center está asociado con cada uno de los grupos de categorías de usuario.

Usuarios de muestra

Durante el despliegue de IBM Intelligent Operations Center, se crean usuarios de muestra.

Los usuarios de muestra genéricos se definen con grupos de roles de usuario y los permisos de acceso correspondientes. Estos usuarios de muestra se definen únicamente como ejemplos y se listan en la tabla siguiente. Se necesitan otros usuarios para administrar la solución.

Tabla 24. Usuarios definidos en IBM Intelligent Operations Center

ID de usuario	Grupo de roles de usuario
Usuarios de muestra	
tdelorne	Ejecutivo en toda la ciudad
scollins	Supervisor en toda la ciudad

Tabla 24. Usuarios definidos en IBM Intelligent Operations Center (continuación)

ID de usuario	Grupo de roles de usuario
akelly	Operador en toda la ciudad
Usuario necesario	
wpsadmin	wpsadmins

Cuando esté listo para definir usuarios para su empresa, suprima sólo los usuarios de muestra. No debe suprimir el usuario wpsadmin. El usuario wpsadmin es fundamental para las tareas de administración asociadas con IBM Intelligent Operations Center. Para obtener más información sobre los usuarios necesarios, consulte el enlace al final de este tema.

Importante: Sustituya la contraseña predeterminada del usuario wpsadmin con una contraseña nueva. Para obtener información sobre la actualización del ID y las contraseñas de usuario administrador del portal, consulte la documentación de WebSphere Portal.

Conceptos relacionados:

"Información de contraseña" en la página 39
Las contraseñas para varios ID de usuario utilizadas en la solución IBM Intelligent Operations Center se definen en el archivo de propiedades de topología. Por razones de seguridad, se deben cambiar las contraseñas predeterminadas que vienen con IBM Intelligent Operations Center .

Tareas relacionadas:

"Supresión de los usuarios de la muestra" en la página 67
El IBM Intelligent Operations Center se envía con usuarios de muestra. Por motivos de seguridad estos usuarios se deben suprimir cuando se haya instalado IBM Intelligent Operations Center en un entorno de producción.

Información relacionada:

Documentación del producto IBM WebSphere Portal 7

Grupos de rol de usuario y permisos de autorización

El conjunto de permisos para acceder a las funciones en IBM Intelligent Operations Center está asociado con cada grupo de rol de usuario.

Un administrador asigna un rol a un usuario haciendo al usuario miembro del grupo de rol de usuario correspondiente. A cada usuario se le asigna la pertenencia a uno o más grupos de rol de usuario.

La tabla siguiente lista los permisos para cada grupo de rol de usuario proporcionados por IBM Intelligent Operations Center. Para cada grupo de rol de usuario, se otorga un permiso de autorización para cada una de las funciones de IBM Intelligent Operations Center.

Tabla 25. Permisos de grupo de rol de usuario asociado y funciones IBM Intelligent Operations Center

Tipo de característica	Nombre caract	Ejecutivo en toda la ciudad	Supervisor en toda la ciudad	Operador en toda la ciudad	wpsadmins

Tabla 25. Permisos de grupo de rol de usuario asociado y funciones IBM Intelligent Operations Center (continuación)

Página	Supervisor: Estado	Permiso de usuario	Permiso de usuario	Ninguno	Permiso de administrador
	Supervisor: Operaciones	Permiso de usuario	Ninguno	Ninguno	Permiso de administrador
	Supervisor: informes	Ninguno	Permiso de usuario	Ninguno	Permiso de administrador
	Operador: Operaciones	Ninguno	Ninguno	Permiso de usuario	Permiso de administrador
	Operador: informes	Ninguno	Ninguno	Permiso de usuario	Permiso de administrador
	Mapa de ubicación	Ninguno	Permiso de usuario	Permiso de usuario	Permiso de administrador
	Administración	Ninguno	Ninguno	Ninguno	Permiso de administrador

Tabla 25. Permisos de grupo de rol de usuario asociado y funciones IBM Intelligent Operations Center (continuación)

Portlet	Estado	Permiso de usuario	Permiso de usuario	Ninguno	Permiso de administrador
	Obtención de detalles de indicador clave de rendimiento	Permiso de usuario	Permiso de usuario	Ninguno	Permiso de administrador
	Notificaciones	Permiso de usuario	Permiso de usuario	Permiso de usuario	Permiso de administrador
	Contactos	Permiso de usuario	Permiso de usuario	Permiso de usuario	Permiso de administrador
	Mapa	Permiso de usuario	Ninguno	Permiso de usuario	Permiso de administrador
	Detalles	Permiso de usuario	Ninguno	Permiso de usuario	Permiso de administrador
	Mis actividades	Permiso de usuario	Permiso de usuario	Permiso de usuario	Permiso de administrador
	Mapa de ubicación	Ninguno	Permiso de usuario	Permiso de usuario	Permiso de administrador
	Informes	Ninguno	Permiso de usuario	Permiso de usuario	Permiso de administrador
	Intelligent Operations Center - Acerca de	Ninguno	Ninguno	Ninguno	Permiso de administrador
	Consolas de administración	Ninguno	Ninguno	Ninguno	Permiso de administrador
	Comprobación de verificación del sistema	Ninguno	Ninguno	Ninguno	Permiso de administrador
	Resumen de permisos de usuario	Ninguno	Ninguno	Ninguno	Permiso de administrador
	Indicadores clave de rendimiento	Ninguno	Ninguno	Ninguno	Permiso de administrador
	Gestor de mapas de ubicación	Ninguno	Ninguno	Ninguno	Permiso de administrador
	Procedimientos operativos estándar	Ninguno	Ninguno	Ninguno	Permiso de administrador
	Script de suceso	Ninguno	Ninguno	Ninguno	Permiso de administrador
	Ejemplo de aplicación de publicación	Ninguno	Ninguno	Ninguno	Permiso de administrador
	Usuarios y grupos	Ninguno	Ninguno	Ninguno	Permiso de administrador

Los permisos de autorización de IBM Intelligent Operations Center se asignan en base a los grupos de Lightweight Directory Access Protocol (LDAP). Los permisos se definen de la manera siguiente:

- El permiso de usuario es la autoridad otorgada a un usuario para darles acceso para visualizar y trabajar con las funciones.

- El permiso de administrador es la autoridad otorgada a un administrador para proporcionarles acceso para:
  - Configurar características
  - Crear, modificar o eliminar usuarios y grupos de usuarios

Para acceder a los datos en IBM Intelligent Operations Center , el usuario debe ser miembro de un grupo de categoría de usuario que proporciona los permisos de datos necesarios.

Conceptos relacionados:

"Resumen de permisos de usuario" en la página 83
Utilice el portlet Resumen de permisos de usuario para ver los permisos asociados con los grupos y usuarios de IBM Intelligent Operations Center .

"Acceso y roles de usuario" en la página 72
El IBM Intelligent Operations Center implementa la seguridad limitando el acceso a las categorías basadas en roles de usuario.

Tareas relacionadas:

"Adición de un nuevo usuario o grupo" en la página 78
Seleccione un grupo y crear un perfil de usuario para agregar un nuevo usuario a IBM Intelligent Operations Center . Seleccione un nombre de grupo para agregar un nuevo grupo.

"Visualización o modificación de la pertenencia a grupos" en la página 80
Vea o modifique la pertenencia a grupos para gestionar los permisos de acceso de usuarios dentro de IBM Intelligent Operations Center.

Referencia relacionada:

"Grupos de categorías de usuarios y permisos de datos"
El permiso para acceder a una categoría de datos en IBM Intelligent Operations Center está asociado con cada uno de los grupos de categorías de usuario.

Información relacionada:

Documentación del producto IBM WebSphere Portal 7

Grupos de categorías de usuarios y permisos de datos

El permiso para acceder a una categoría de datos en IBM Intelligent Operations Center está asociado con cada uno de los grupos de categorías de usuario.

Un administrador asigna el acceso a datos a un usuario haciendo al usuario miembro del grupo de rol de usuario correspondiente. A cada usuario se le asigna la pertenencia a uno o más grupos de categoría de usuario.

La siguiente lista enumera las categorías de datos cubiertas por IBM Intelligent Operations Center y los grupos de categorías de usuario correspondientes para identificar sucesos, indicadores clave de rendimiento (KPI) y datos de alerta. Por ejemplo, si un usuario quiere poder ver los sucesos relacionados con el departamento de agua de la ciudad, el usuario tiene que ser miembro del grupo `ioc_base_infrastructure`.

Tabla 26. Identificadores y descripciones de grupo de categorías de usuario

Categoría de datos	Descripción	Grupo de categorías de usuario
CBRNE	Amenaza o ataque químico, biológico, radiológico, nuclear o explosivos de alto rendimiento	`ioc_base_chemical, ioc_base_biological, ioc_base_radiological, ioc_base_nuclear, ioc_base_explosive`
Ent.	Ambiental: contaminación y otros problemas ambientales	`ioc_base_environmental`

Tabla 26. Identificadores y descripciones de grupo de categorías de usuario (continuación)

Categoría de datos	Descripción	Grupo de categorías de usuario
Incendio	Extinción de incendios y rescate	`ioc_base_fire`
Geo	Geofísico (Incluyendo derrumbes)	`ioc_base_geophysical`
Salud	Medicina y salud pública	`ioc_base_health`
Infra	Infraestructura: Servicios, telecomunicaciones, otras infraestructuras que no son de transporte	`ioc_base_infrastructure`
Cumplido	Meteorológica (incluyendo inundaciones)	`ioc_base_meteorological`
Rescate	Rescate y recuperación	`ioc_base_rescue`
Seguridad	Emergencia general y seguridad pública	`ioc_base_safety`
Seguridad	Seguridad local y privada, nacional, militar y cumplimiento de la ley	`ioc_base_security`
Transporte	Transporte público y privado	`ioc_base_transportation`
Otros	Otros sucesos, KPI o alertas	`ioc_base_other`

Para iniciar sesión y acceder a las características de IBM Intelligent Operations Center, un usuario debe ser miembro de un grupo de rol que proporciona los permisos de autorización requeridos.

Conceptos relacionados:

"Resumen de permisos de usuario" en la página 83
Utilice el portlet Resumen de permisos de usuario para ver los permisos asociados con los grupos y usuarios de IBM Intelligent Operations Center .

"Acceso y roles de usuario" en la página 72
El IBM Intelligent Operations Center implementa la seguridad limitando el acceso a las categorías basadas en roles de usuario.

Tareas relacionadas:

"Adición de un nuevo usuario o grupo"
Seleccione un grupo y crear un perfil de usuario para agregar un nuevo usuario a IBM Intelligent Operations Center . Seleccione un nombre de grupo para agregar un nuevo grupo.

"Visualización o modificación de la pertenencia a grupos" en la página 80
Vea o modifique la pertenencia a grupos para gestionar los permisos de acceso de usuarios dentro de IBM Intelligent Operations Center.

Referencia relacionada:

"Grupos de rol de usuario y permisos de autorización" en la página 74
El conjunto de permisos para acceder a las funciones en IBM Intelligent Operations Center está asociado con cada grupo de rol de usuario.

Información relacionada:

Documentación del producto IBM WebSphere Portal 7

Adición de un nuevo usuario o grupo

Seleccione un grupo y crear un perfil de usuario para agregar un nuevo usuario a IBM Intelligent Operations Center . Seleccione un nombre de grupo para agregar un nuevo grupo.

Acerca de esta tarea

Primero, seleccione un grupo de roles de usuario para configurar el nivel correcto de permisos de acceso al añadir un nuevo usuario. A continuación, complete los campos de la página **Gestión de perfil** para

que IBM Intelligent Operations Center tenga la información necesaria a añadir en el nuevo usuario. Siga el enlace al final del tema para obtener más información acerca de lo que puede entrar en los campos de la página **Gestión de perfil** .

Procedimiento

1. Inicie sesión en `http://host-apl/wpsv70/wps/myportal/` como usuario administrativo.
2. Pulse **Administración** en la barra de navegación en la parte superior de la página.
3. Pulse **Acceso** en el menú de la barra lateral.
4. Pulse **Usuarios y grupos** en el submenú.
5. Si va a añadir un usuario nuevo, seleccione un rol dándole la permanencia de usuario de un grupo. Busque el grupo pulsando **Todos los grupos de usuario del portal** para obtener una lista de grupos y pulse el grupo que necesite.
6. Pulse **Nuevo usuario** o **Nuevo grupo**.
7. Si está creando un grupo de usuarios, entre un nombre para el grupo de usuarios.
8. Si está añadiendo un usuario nuevo, asegúrese de que entra todos los campos necesarios en el perfil de usuario como indican los asteriscos.
9. Pulse **Aceptar** para enviar el nuevo perfil o grupo.

Resultados

Un mensaje confirma si el envío es correcto. Se crea y se muestra un nuevo perfil de usuario en la lista de grupo o se muestra un grupo nuevo. El nuevo usuario está autorizado a acceder a IBM Intelligent Operations Center según los permisos asignados al grupo de rol seleccionado.

Qué hacer a continuación

- Proporcione al nuevo usuario la pertenencia de grupos de categoría de datos según los permisos de datos requeridos.
- Si se ha añadido un grupo nuevo, añada el grupo al ACL de unión de WebSphere Application Server Network Deployment .
- Si se ha añadido un grupo nuevo, los permisos de autorización también deben establecerse para el grupo. Los permisos de autorización definen qué funciones y miembros de datos del grupo se pueden ver y modificar. Para obtener información sobre la configuración de permisos de autorización, consulte el enlace a la documentación de IBM WebSphere Portal 7, situado al final de este tema, y busque la información sobre la asignación de acceso a páginas.
- Asigne el nuevo usuario a un grupo de seguridad y grupo de personas en Tivoli Service Request Manager.

Nota: Para ahorrar tiempo se pueden duplicar las asignaciones de grupo para un usuario nuevo sobre la base de un usuario existente. Seleccione el nuevo usuario y pulse en el icono **Duplicar** . Seleccione el usuario existente para duplicar la pertenencia a grupos.

Conceptos relacionados:

"Acceso y roles de usuario" en la página 72
El IBM Intelligent Operations Center implementa la seguridad limitando el acceso a las categorías basadas en roles de usuario.

Tareas relacionadas:

"Configuración de nuevos usuarios en Tivoli Service Request Manager" en la página 130
Cuando añade un usuario a IBM Intelligent Operations Center, asigna permisos y grupos de personas para el usuario en Tivoli Service Request Manager.

Referencia relacionada:

"Grupos de rol de usuario y permisos de autorización" en la página 74
El conjunto de permisos para acceder a las funciones en IBM Intelligent Operations Center está asociado con cada grupo de rol de usuario.

"Grupos de categorías de usuarios y permisos de datos" en la página 77
El permiso para acceder a una categoría de datos en IBM Intelligent Operations Center está asociado con cada uno de los grupos de categorías de usuario.

Información relacionada:

Documentación del producto IBM WebSphere Portal 7

Visualización o modificación de la pertenencia a grupos

Vea o modifique la pertenencia a grupos para gestionar los permisos de acceso de usuarios dentro de IBM Intelligent Operations Center.

Acerca de esta tarea

Seleccione el grupo correspondiente al rol o categoría de datos para el que desea ver o cambiar la pertenencia. La pertenencia a un grupo de roles proporciona a los usuarios el acceso a las partes de la solución apropiada para ese rol. La pertenencia a un grupo de categorías proporciona a los usuarios el acceso a los sucesos, los indicadores clave de rendimiento (KPI) y las alertas asociadas a esa categoría.

Pase el ratón sobre un icono para ver la ayuda contextual que indica el propósito del icono.

Procedimiento

1. Inicie sesión en `http://host-apl/wpsv70/wps/myportal/` como usuario administrativo.
2. Pulse **Administración** en la barra de navegación en la parte superior de la página.
3. Pulse **Acceso** en el menú de la barra lateral.
4. Pulse **Usuarios y grupos** en el submenú.
5. Pulse **Todos los Grupos de usuarios del portal** para mostrar una lista de los grupos y pulse el grupo que necesite. Los miembros del grupo se enumeran.
6. Puede realizar las siguientes acciones en relación con la pertenencia a grupos:
   - Ver la pertenencia a otros grupos pulsando **Ver pertenencia** para el ID de usuario.
   - Agregar un usuario o usuarios al grupo pulsando **Añadir miembro** y seleccionando el usuario o usuarios que va a añadir.
   - Eliminar un usuario del grupo pulsando **Quitar** para el ID de usuario.

Referencia relacionada:

"Grupos de rol de usuario y permisos de autorización" en la página 74
El conjunto de permisos para acceder a las funciones en IBM Intelligent Operations Center está asociado con cada grupo de rol de usuario.

"Grupos de categorías de usuarios y permisos de datos" en la página 77
El permiso para acceder a una categoría de datos en IBM Intelligent Operations Center está asociado con cada uno de los grupos de categorías de usuario.

Información relacionada:

Documentación del producto IBM WebSphere Portal 7

Visualización o edición de su perfil de usuario

Ver o editar el perfil de un usuario para establecer o restablecer cualquiera de los atributos del perfil de usuario incluyendo la contraseña. No puede cambiar el ID de usuario.

Acerca de esta tarea

Seleccione el usuario de una lista autenticada de usuarios del portal para abrir el perfil de usuario y cambiar detalles el perfil. Cada usuario también puede cambiar su propio perfil.

Pase el ratón sobre un icono para ver la ayuda contextual que indica el propósito del icono.

Procedimiento

1. Inicie sesión en `http://host-apl/wpsv70/wps/myportal/` como usuario administrativo.
2. Pulse **Administración** en la barra de navegación superior.
3. Pulse el elemento **Acceso** en el menú de la barra lateral.
4. Pulse **Usuarios y grupos** en el submenú.
5. Pulse **Todos los usuarios del portal autenticados** para mostrar una lista de usuarios.
6. Haga clic en el icono de edición para el usuario para mostrar la página **Gestión de perfiles** . Se visualizan los campos de atributo para el perfil de usuario.
7. Si desea cambiar la contraseña, entre una contraseña nueva en los campos **Nueva contraseña:** y **Confirmar contraseña:** .
8. Puede introducir, modificar o eliminar la información en cualquiera de los campos restantes.
9. Pulse **Aceptar** para enviar los cambios que ha realizado.

Resultados

El perfil de usuario se actualiza con los cambios presentados.

Información relacionada:

Documentación del producto IBM WebSphere Portal 7

Supresión de un usuario o grupo

Suprima un usuario o grupo de IBM Intelligent Operations Center.

Acerca de esta tarea

Para suprimir un usuario, seleccione el usuario de la lista de usuarios del portal autenticados y elimínelo. Para suprimir un grupo, seleccione el grupo de la lista de grupos de usuario del portal y elimínelo.

Pase el ratón sobre un icono para ver la ayuda contextual que indica el propósito del icono.

Nota: Tenga en cuenta que al suprimir un usuario de IBM Intelligent Operations Center también se elimina su acceso a otras soluciones dentro de la familia de productos IBM Smarter Cities™ Software Solutions. La supresión de un grupo también elimina ese grupo de otras soluciones.

Procedimiento

1. Inicie sesión en `http://host-apl/wpsv70/wps/myportal/` como usuario administrativo.
2. Pulse **Administración** en la barra de navegación superior.
3. Pulse **Acceso** en el menú de la barra lateral.
4. Pulse **Usuarios y grupos** en el submenú:
   - Pulse **Todos los Grupos de usuarios del portal** para mostrar una lista de los grupos.
   - Pulse **Todos los usuarios del portal autenticados** para mostrar una lista de usuarios.
5. Pulse el icono **Suprimir** correspondiente al usuario o grupo que desea suprimir.

Resultados

El usuario o grupo que suprime ya no existen en IBM Intelligent Operations Center. La supresión de un grupo no suprime a los miembros del grupo.

Información relacionada:

Documentación del producto IBM WebSphere Portal 7

Importación de usuarios y grupos

Puede importar usuarios en bloque a IBM Intelligent Operations Center a través del servicio del portal.

Acerca de esta tarea

Como administrador del portal, puede importar usuarios en bloque a IBM Intelligent Operations Center a través de la consola de administración del portal. El archivo XML necesario para esta tarea se puede encontrar en servidor de aplicaciones: `/opt/IBM/WebSphere/PortalServer/doc/xml-samples/CreateUser.xml`. Este archivo XML se puede modificar para añadir usuarios a IBM Intelligent Operations Center.

Nota: Al añadir varios usuarios, añada todos los usuarios primero, antes de añadirlos a los grupos. Consulte el ejemplo que encontrará al final del tema.

Como alternativa al siguiente procedimiento, puede ejecutar desde la línea de mandatos el script `xmlaccess.sh` ubicado en servidor de aplicaciones.

Procedimiento

1. Actualice el archivo `CreateUser.xml` para que contenga los usuarios nuevos y los grupos a los que pertenecen.
2. Inicie sesión en http://*host-apl*/wpsv70/wps/myportal/ como un usuario administrativo.
3. Pulse **Administración**.
4. En **Configuración del portal**, pulse **Importar XML**.
5. Navegue al archivo XML actualizado.
6. Pulse en **Importar**.

Resultados

WebSphere Portal Server crea de forma automática las entradas asociadas en el directorio en Tivoli Directory Server y en Tivoli Access Manager WebSEAL.

Ejemplo

El ejemplo siguiente modifica el archivo XML para añadir dos usuarios a IBM Intelligent Operations Center y para añadir cada uno de ellos a un grupo de roles y a un grupo de categorías:

```
<?xml version="1.0" encoding="UTF-8"?>
<request xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="PortalConfig_7.0.0.xsd" type="update"
create-oids="true">
<portal action="locate">
<user action="update" name="cityuser003" firstname="City"
lastname="user003" password="passw0rd">
<parameter name="preferredLanguage" type="string"
update="set">en_US</parameter>
<parameter name="cn" type="string" update="set">City user003</parameter>
</user>
<user action="update" name="cityuser004" firstname="City"
lastname="user003" password="passw0rd">
<parameter name="preferredLanguage" type="string"
update="set">en_US</parameter>
<parameter name="cn" type="string" update="set">City user004</parameter>
</user>
<group action="update" name="City Executive">
<member-user update="set" id="cityuser003">
</group>
<group action="update" name="ioc_base_fire">
<member-user update="set" id="cityuser003">
<group action="update" name="City Executive">
<member-user update="set" id="cityuser004">
</group>
<group action="update" name="ioc_base_fire">
<member-user update="set" id="cityuser004">
</group>
</portal>
</request>
```

Conceptos relacionados:

"Consolas de administración" en la página 207
Utilice el portlet Consolas de administración para administrar los servicios proporcionados por la solución.

Información relacionada:

Documentación del producto IBM WebSphere Portal 7

Information Center de Tivoli Directory Server

Information Center de Tivoli Access Manager

Resumen de permisos de usuario

Utilice el portlet Resumen de permisos de usuario para ver los permisos asociados con los grupos y usuarios de IBM Intelligent Operations Center .

El portlet Resumen de permisos de usuario visualiza detalles sobre pertenencia a grupos y permisos otorgados a los usuarios.

Para acceder al portlet Resumen de permisos de usuario, en la interfaz de administración de WebSphere Portal haga clic en **Intelligent Operations** > **Herramientas de administración** > **Resumen de permisos de usuario**.

Utilice la pestaña **Usuario** para comprobar los permisos para un usuario. Entre un ID de usuario para ver la siguiente información:

- Una lista completa de todas las categorías de datos y grupos de categoría de usuario está disponible en IBM Intelligent Operations Center.
- Una lista de los permisos de categoría de datos asignados al usuario especificado.
- Una lista de todos los grupos, grupos de rol de usuario y grupos de categoría de usuario de los que es miembro el usuario especificado.
- Una lista de cada categoría de datos indica si el usuario especificado tiene permiso para esa categoría.

Utilice la pestaña **Resumen** ficha para ver estadísticas de resumen correspondientes a usuarios y permisos de grupo. Puede visualizar la siguiente información:

- Número total de grupos en IBM Intelligent Operations Center.
- Número total de usuarios autorizados para acceder a IBM Intelligent Operations Center.
- Lista del número total de usuarios por categoría de datos.
- Lista del número total de usuarios por grupo de rol de usuario.

Referencia relacionada:

"Grupos de rol de usuario y permisos de autorización" en la página 74
El conjunto de permisos para acceder a las funciones en IBM Intelligent Operations Center está asociado con cada grupo de rol de usuario.

"Grupos de categorías de usuarios y permisos de datos" en la página 77
El permiso para acceder a una categoría de datos en IBM Intelligent Operations Center está asociado con cada uno de los grupos de categorías de usuario.

Descripción general de Cyber Hygiene

La función Cyber Hygiene de IBM Intelligent Operations Center está diseñada para proporcionar servicios que solucionen exposiciones de seguridad potenciales en el sistema instalado.

Nota: Normalmente, el término "vulnerabilidad" se utiliza para hacer referencia tanto a las vulnerabilidades de seguridad como a las exposiciones de seguridad. Cyber Hygiene define una vulnerabilidad como un error de programación en una aplicación que permite brechas de seguridad. Cyber Hygiene define una exposición como una selección de configuración de sistema operativo o aplicación que es poco segura. Las exposiciones se pueden abordar seleccionando una opción de configuración más segura. Por ejemplo, se puede configurar un directorio para permitir que todos los usuarios almacenen archivos en él. También se puede configurar de forma más segura para que sólo pueda almacenar archivos en el directorio el propietario.

Cyber Hygiene tiene dos elementos clave:

- Mitigación y corrección de exposiciones de seguridad conocidas en el sistema operativo Linux y los usuarios, directorios y archivos asociados. Lo hace a través de un conjunto de herramientas y scripts.
- Documentación de la evaluación de casi 1000 vulnerabilidades y exposiciones conocidas en la configuración del sistema operativo, productos y sistema.

Al manejar las exposiciones de seguridad durante el proceso de instalación, el cliente se ahorrará trabajo a la hora de alcanzar un nivel de seguridad mayor en el sistema desplegado.

Por ejemplo, una agencia gubernamental puede utilizar la remediación y la documentación de Cyber Hygiene para facilitar la certificación y acreditación del sistema para el despliegue en una red protegida. Los clientes de negocios comerciales pueden utilizar el mismo proceso para mejorar la seguridad de sus entornos.

Cyber Security proporciona migración de riesgo, no prevención de riesgo. Dado que los sistemas se tienen que ejecutar y tienen que ser accesibles para proporcionar valor, siempre hay riesgo de que se pueda comprometer la información de un sistema o su control.

Cyber Hygiene no direcciona vulnerabilidades específicas de aplicaciones que incluyen cómo la aplicación maneja amenazas como Denegación de servicio, inyección de SQL, etc. En lugar de eso, Cyber Hygiene proporciona una base para la seguridad de las aplicaciones direccionando las exposiciones de seguridad de usuario, directorio y archivo de forma general; no destinadas a ninguna aplicación específica. Cyber Hygiene se ejecuta después de la instalación del producto para corregir las vulnerabilidades generales del sistema y de usuarios de aplicación, directorios y archivos. Cualquier aplicación utilizada con el sistema operativo Linux tiene que evaluarse de manera separada para las vulnerabilidades específicas de la aplicación.

El catálogo de vulnerabilidades y exposiciones conocidas y utilizadas en Cyber Hygiene se basa en listas de comprobación sin clasificar y no confidenciales de la United States Defense Information Services Agency (DISA). Los elementos de estas listas se evalúan para su aplicación a Cyber Hygiene. Los scripts de análisis buscan y registran instancias de una exposición y, a continuación, cuando convenga, los archivos de registro se utilizan como entrada para los scripts de remediación que direccionan el problema. Un pequeño subconjunto de hallazgos de seguridad requiere diferente gestión.

El listado de documentación sobre vulnerabilidades conocidas en componentes deIBM Intelligent Operations Center y las acciones llevadas a cabo por Cyber Hygiene para mitigarlas, lo proporcionaIBM Intelligent Operations Center.

Tareas relacionadas:

"Lista de comprobación - instalación utilizando IBM Installation Manager" en la página 14
Utilice la lista de comprobación para rastrear los pasos de instalación al instalar IBM Intelligent Operations Center utilizando IBM Installation Manager.

"Lista de comprobación - instalación paso a paso" en la página 16
Utilice esta lista de comprobación para hacer un seguimiento de los pasos de instalación al instalar IBM Intelligent Operations Center utilizando scripts y mandatos.

"Instalación de IBM Intelligent Operations Center utilizando Installation Manager" en la página 26
IBM Intelligent Operations Center puede instalarse utilizando el instalador gráfico proporcionado.

"Instalación y ejecución paso a paso de Cyber Hygiene" en la página 62
Cyber Hygiene se ha instalado y ejecutado por separado de IBM Intelligent Operations Center y se debe instalar y ejecutar cuando todos los componentes de IBM Intelligent Operations Center estén instalados, configurados y en funcionamiento. Cyber Hygiene cambia la configuración predeterminada del sistema operativo a un conjunto de opciones más seguras para proteger el sistema IBM Intelligent Operations Center.

Ciber-seguridad

Asegurar los entornos de TI ha sido durante muchos años un problema para los gobiernos nacionales y es cada vez más importante en relación con sistemas de infraestructuras críticos. En los productos y soluciones que proporcionan infraestructuras críticas, como IBM Intelligent Operations Center, se debe, siempre que sea posible, eliminar las vulnerabilidades conocidas antes de que estos productos y soluciones estén disponibles.

La ciber-seguridad es la mitigación de riesgos, no la prevención de los mismos. Dado que los sistemas de TI se tienen que ejecutar y tienen que ser accesibles para proporcionar valor, siempre hay riesgo de que se pueda comprometer la información de un sistema o su control.La ciber-seguridad incluye tanto los elementos estáticos como los dinámicos. Cyber Hygiene de IBM Intelligent Operations Center se encarga de los elementos estáticos de la ciber-seguridad. Para hacerse cargo de los elementos dinámicos de la ciber-seguridad también se requieren otras herramientas y procesos. Entre estas herramientas y procesos se pueden incluir procedimientos de seguridad físicos y personales o herramientas de intrusión en redes.

Las prestaciones de Cyber Hygiene proporcionadas por IBM Intelligent Operations Center están diseñadas para hacerse cargo de áreas como configuraciones de seguridad débiles, errores de software, errores de administración de sistemas y errores de procesos de seguridad de los sistemas. Para proporcionar este soporte, Cyber Hygiene proporciona características de instalación y configuración que

configuran el sistema operativo y características de administración que definen los ajustes seguros e instala fixpacks de seguridad fundamentales. Por ejemplo, los sistemas se configuran de forma que no existan ID de usuario sin contraseña y los servicios Linux poco seguros como ftp, snmp, rlogin estén inhabilitados. No obstante, los sistemas no se pueden configurar automáticamente para adaptarse a prácticas de seguridad empresariales específicas.

Listas de comprobación de Cyber Hygiene

Cyber Hygiene utiliza listas de comprobación basadas en listas sin restricciones y alertas de vulnerabilidades periódicas de la Defense Information Systems Agency (DISA).

Análisis de elementos de la lista de comprobación

Cada vulnerabilidad identificada en la lista de comprobación sin restricciones de la Defense Information System Agency (DISA) define los datos relacionados con la vulnerabilidad.

La información proporcionada para cada vulnerabilidad incluye lo siguiente:

- Un identificador exclusivo. El identificador está formado por un ID de la Guía técnica de implementación de seguridad (STIG) y una clave del Sistema de gestión de vulnerabilidades (VMS).
- Un nombre corto que resume la vulnerabilidad.
- La gravedad de la vulnerabilidad. Entre los niveles de gravedad se encuentran los siguientes:

  I Gravedad alta

  II Gravedad media

  III Gravedad baja
- El producto o productos afectado(s).
- La versión o versiones de los productos afectada(s).
- Una descripción de la vulnerabilidad, incluyendo casos de uso, contexto o interacciones con otros software.
- Toda acción recomendada. Si la corrección no está disponible a través de un parche o actualización, puede incluirse una mitigación recomendada.
- Cualquier alerta que sustituya a la alerta.

Para cada vulnerabilidad, es importante comprender si afecta o no a IBM Intelligent Operations Center. Por ejemplo:

- ¿El release y nivel de arreglo del producto se incluye con el IBM Intelligent Operations Center afectado? Un release o arreglo anterior podría no estar afectado ya que el problema podría haberse introducido en un release o arreglo posterior.
- ¿El producto se incluye con el IBM Intelligent Operations Center utilizado de algún modo que queda expuesto a la vulnerabilidad? Por ejemplo, un problema podría existir únicamente si el producto utiliza servicios de otro producto. Si dichos servicios no se utilizan en la configuración de IBM Intelligent Operations Center, esta corrección podría no ser necesaria.
- ¿la vulnerabilidad del producto afecta al sistema operativo utilizado? Algunas vulnerabilidades solo existen al ejecutar sistemas operativos específicos.

Para cada elemento o lista de comprobación, estos factores se han analizado con el fin de determinar la acción necesaria paraIBM Intelligent Operations Center. Este análisis y corrección resultan en una de las cuatro evaluaciones siguientes:

No aplicable (NA)
: El producto o configuración afectados no forman parte del entorno de IBM Intelligent Operations Center.

Sin hallazgos (NF)
: La versión y nivel de arreglo instalados del producto no están afectados o el producto no se

utiliza de forma que quede expuesto a la vulnerabilidad. Esta evaluación también se utiliza si la configuración no está expuesta a la vulnerabilidad.

Abierta
La vulnerabilidad se aplica a la versión y nivel de arreglo del producto instalados, sin embargo, no existe corrección disponible para el producto. Esta evaluación también se utiliza si el sistema está configurado de forma que queda expuesto a la vulnerabilidad.Por ejemplo, permitir permisos de escritura global en un directorio porque un producto lo requiere... Esta evaluación se utiliza también cuando se aplica a una corrección que podría depender de políticas de organización como políticas de contraseñas basadas en una combinación de caracteres o en la longitud.

Solucionada
Se ha aplicado y verificado una corrección de una vulnerabilidad abierta.

Tabla 27 muestra un análisis de ejemplo. El segundo ejemplo muestra el manejo de un producto que no está instalado en ningún servidor de IBM Intelligent Operations Center.

Tabla 27. Evaluaciones de vulnerabilidades de ejemplo

ID	Nombre	Gravedad	Servidor de aplicaciones	Servidor de sucesos	Servidor de datos	Servidor de gestión	Explicación
2011-B-0082	Varias vulnerabilidades en IBM Websphere Application Server	I	NF	Abierta	NA	NF	Afecta a versiones anteriores a las versiones 6.1.0.39 y 7.0.0.19
2011-B-0085	Varias vulnerabilidades de denegación de servicio en Wireshark	I	NA	NA	NA	NA	Wireshark no está instalado

Selección de lista de comprobación

Las listas de comprobación utilizadas para cada servidor se basan en el software instalado en ese servidor. Las listas de comprobación específicas se encargan de vulnerabilidades para tipos de productos, por ejemplo bases de datos. Otras están dirigidas a productos específicos de una categoría, por ejemplo DB2.

No todos los tipos de productos tienen listas de comprobación específicas. Las vulnerabilidades genéricas están documentadas en la lista de comprobación Seguridad de la aplicación o en una lista relacionada con el sistema operativo.

Cyber Hygiene utiliza los siguientes tipos de listas de comprobación:

Seguridad de la aplicación
Indica las vulnerabilidades a nivel del sistema. Algunas están relacionadas con el desarrollo de software y las prácticas de comprobación, mientras que otras lo están con vulnerabilidades específicas de la aplicación como la falta de uso de contraseñas cifradas durante la autenticación del usuario.

Unix/Linux
Indica las vulnerabilidades relacionadas con la configuración, gestión de contraseñas, particionamiento del sistema de archivos, etc.

Servidor web
Indica las vulnerabilidades relacionadas con los servidores HTTP.

Base de datos
Indica las vulnerabilidades relacionadas con los servidores de bases de datos.

Servidores de directorios
Indica las vulnerabilidades relacionadas con los servidores LDAP.

Gestión de sistemas empresariales
Indica las vulnerabilidades relacionadas con las herramientas de gestión de sistemas empresariales y los procesos de gestión de sistemas.

Las listas de comprobación no se encargan de la seguridad de la red puesto que la configuración de esta debe ser determinada por las políticas y arquitectura de red del cliente. La configuración de la seguridad de la red debe realizarse de acuerdo con las necesidades de cada instalación.

Configuración predeterminada de Cyber Hygiene

La característica Cyber Hygiene establece configuraciones y políticas predeterminadas de Linux a opciones más seguras de las establecidas en la instalación predeterminada del sistema operativo.Los administradores del sistema pueden modificar fácilmente la configuración predeterminada para que la instalación cumpla las políticas de seguridad.

El grupo administrativo de operaciones de TI de la empresa será el responsable de la seguridad de los sistemas. Esto incluye la gestión del acceso a la red y las políticas y procesos de seguridad internos.

Cuando la configuración predeterminada de Cyber Hygiene se incoherente con las políticas empresariales, estas últimas serán las que prevalecerán. Recuerde que el impacto de la configuración de las políticas de seguridad locales en las funcionalidades del sistema no se ha comprobado. Asimismo, ha de tener cuidado al aplicar las políticas de seguridad a productos no desplegados con Cyber Hygiene al aplicar las mismas a IBM Intelligent Operations Center.

Mientras que IBM Intelligent Operations Center no se puede configurar automáticamente para políticas de seguridad empresariales individuales, IBM Intelligent Operations Center se puede configurar de forma que elimine las vulnerabilidades conocidas. Cyber Hygiene configura IBM Intelligent Operations Center con una serie de políticas de prácticas adecuadas predeterminadas para crear una base para que los administradores del sistema puedan utilizar al aplicar prácticas y políticas de organización específicas

Políticas de gestión de contraseña predeterminada

Cyber Hygiene configura las políticas de gestión de contraseñas del sistema operativo Linux.

Las políticas de gestión de contraseñas predeterminadas establecidas por Cyber Hygiene se muestran en Tabla 28.

Tabla 28. Políticas de gestión de contraseñas de Cyber Hygiene predeterminadas

Política	**Valor o configuración**
Longitud mínima de la contraseña	8 caracteres
Caracteres aceptados	letras mayúsculas, letras minúsculas, números, caracteres especiales (: ;! ` ~ @ # $ % ^ & * ( ) - _ = + [{] } \ | ' " , < . > / ? y el carácter de espacio)
Reglas de contenido	ninguno
Número de registros fallidos en intentos antes de la desconexión de seguridad del usuario	3
Tiempo mínimo entre los cambios de contraseñas	1 día
Tiempo máximo entre los cambios de contraseñas	60 días
¿Son necesarias las contraseñas de las cuentas?	sí
¿Cuándo se puede volver a utilizar una contraseña?	después de 5 contraseñas diferentes
Inicio de sesión necesario después de inactividad	15 minutos de inactividad
Demora entre anomalías de inicio de sistema	4 segundos

Los archivos `/etc/pam.d/system-auth` y `/etc/login.defs` se modifican al establecer las políticas predeterminadas de Cyber Hygiene.

Estos ajustes están destinados a ser el mínimo necesario para prácticas de seguridad razonables. Debe modificar estos valores para que coincidan con las políticas de seguridad de la organización.A continuación se indican algunas áreas en las que podría querer cambiar la configuración predeterminada:

- Mientras que la configuración predeterminada define la longitud mínima de las contraseñas en 8 caracteres, las prácticas adecuadas de sistemas seguros generalmente consideran que las contraseñas son más seguras con una longitud de 14 o más caracteres.
- El tiempo máximo entre cambios de contraseña debe definirse con un valor adecuado para su organización. Este se define en el parámetro**inactive** del archivo `/etc/shadow`. En el momento definido, el usuario se verá obligado a cambiar la contraseña al iniciar sesión. Si el usuario no cambia la contraseña, está deberá ser restablecida por un usuario privilegiado. Si se utiliza el valor identificado en el archivo `/etc/shadow` depende de la acción predeterminada especificada en el archivo`/etc/default/useradd`. Si el archivo `/etc/default/useradd` especifica -1, la contraseña no caducará. Si `/etc/default/useradd` especifica 0, la cuenta está bloqueada. Si se define cualquier otro valor en el archivo `/etc/default/useradd`, el valor del parámetro**inactive** de `/etc/shadow` se utilizará para la caducidad de la contraseña.
- Las reglas relacionadas con la complejidad y contenido de las contraseñas se deben establecer e implementar de acuerdo con la política de seguridad de la empresa.

Consulte la documentación de Linux para obtener más información sobre la gestión de las políticas de contraseña.

Servicios de Linux inhabilitados

Cyber Hygiene deshabilita o desinstala los servicios de Linux más vulnerables.Estos servicios pueden permitir el acceso al sistema y solo deben iniciarse o instalarse si existe necesidad.

Los siguientes servicios Linux (daemons) no se inician de forma predeterminada. Se puede iniciar si es necesario.

- inetd/xinetd
- portmap
- avahi-daemon
- bluetooth
- cups
- hidd
- isdn
- rhnsd
- canna
- pcmcia
- ypbind
- autofs
- smartd
- netfs
- snmpd
- nfs
- samba

Estos servicios se pueden iniciar utilizando el mandato **service** *service_name* **start** .

Nota: Estos servicios, si no se configuran correctamente, se pueden comprometer y permitir accesos no autorizado al sistema. Esto es por lo que, por seguridad del sistema, no se inician de forma predeterminada.

Se eliminan los siguientes servicios Linux. En caso de ser necesario, se pueden volver a instalar utilizando los mandatos **rpm** o **yum**. Por ejemplo, el mandato **yum install httpd** instalará el paquete de daemon HTTP.

- tcpdump
- sendmail
- squid
- vnc-server
- httpd
- mod_python
- mod_perl
- mod_ssl
- webalizer
- httpd-manual

Nota: Estos servicios se eliminan de Linux porque tienen un alto potencial para provocar exposiciones de seguridad en entornos de servidores.

ID de usuario eliminados

Una instalación estándar de Linux contiene un número de ID de usuario que no son deseables en un entorno de producción seguro. Cyber Hygiene elimina estos ID de usuario del registro de usuarios de Linux y del archivo `/etc/passwd`.Los siguientes directorios de inicio asociados también se eliminan.

Los siguientes ID de usuario se eliminan y se puede volver a crear si es necesario.

- juegos
- noticias
- ftp
- parada
- apagado
- reinicio
- quién
- gopher
- lp
- rpcuser
- uucp

Si se necesitan estos ID de usuario, se pueden utilizar los procedimientos de administración estándar de Linux para crearlos.

Reglas de auditoría

Las auditoría estándar en Linux son mínimas ya que los archivos de auditoría pueden aumentar rápidamente. No obstante, cuando la seguridad se ve afectada, las auditorías adicionales son fundamentales para poder determinar lo ocurrido en un incidente. Los scripts de Cyber Hygiene añaden un conjunto de reglas de auditoría adicionales a todos los niveles de ejecución de Linux. Los sucesos que coinciden con estas reglas se iniciarán en los archivos de registro del sistema estándar.

Se añaden las siguientes reglas de auditoría de Linux y se pueden modificar si fuera necesario.

- Intentos fallidos de acceso a programas y archivos
- Supresión de programas y archivos
- Acciones privilegiadas, de seguridad y administrativas
- Cambios de permiso del control de acceso

Tener buenos registros de auditoría es una buena práctica de seguridad. Si, por algún motivo, la auditoría definida por Cyber Hygiene se debe cambiar, los archivos `/etc/audit/auditd.conf` y `/etc/audit/audit.rules` se deben modificar. Cyber Hygiene activa la auditoría en los cinco niveles de tiempo de ejecución de Red Hat Enterprise Linux.

Permisos de archivo y de directorio

Cyber Hygiene cambia los permisos de archivo y directorio existentes para que cumplan las buenas prácticas de seguridad.

Los cambios en los permisos de archivos y directorios realizados por Cyber Hygiene son los siguientes:

Restricción de script del sistema

Los usuarios no pueden acceder a los script del sistema de seguridad sin privilegios adecuados.

Retirada del permiso de escritura en todo el mundo

Los usuarios no pueden escribir a directorios que no son públicos. La obligación de los usuarios y aplicaciones para modificar archivos y directorios debe ser el propietario o un miembro del grupo para el archivo o directorio.

Eliminación de permisos de ejecución y lectura a nivel mundial

Los permisos ejecutables y legibles a nivel mundial se eliminan para muchos archivos y directorios. En concreto, estos permisos se eliminan de los directorios de inicio de los usuarios. La obligación de los usuarios y aplicaciones para leer o ejecutar archivos debe ser el propietario o un miembro del grupo para el archivo o directorio.

Otros cambios

Cyber Hygiene realiza otros cambios para hacer frente a exposiciones de seguridad.

Programas por lotes - mandato `at`

Para impedir que los usuarios sin privilegios utilicen el mandato **`at`** para ejecutar programas de lotes a una hora determinada, Cyber Hygiene suprime el archivo `at.deny` y crea un archivo `at.allow` vacío.

El archivo `at.allow` define los usuarios que tiene permiso para ejecutar el mandato **`at`**. Un archivo `at.allow` que no contenga ID de usuario indica que no hay usuarios, exceptuando los ID del sistema con privilegios, que puedan ejecutar el mandato **`at`**. Si existe el archivo `at.deny`, que define los usuarios que no tiene permiso de forma explícita para utilizar el mandato**`at`**, pero no existe el archivo `at.allow`, todos los usuarios, excepto los indicados en el archivo`at.deny`, podrán ejecutar el mandato **`at`**. Si no existe ninguno de los archivos, el mandato**`at`** solo podrá ser ejecutado por el superusuario.

De forma predeterminada, Red Hat Enterprise Linux está configurado para permitir la ejecución del mandato**`at`**.

Programas por lotes - mandato `cron`

Los usuarios sin privilegios administrativos no puede ejecutar el mandato **`cron`** para planificar programas por lotes.

Control-Alt-Supr

La combinación de teclas Ctrl-Alt-Supr está inhabilitada y no se puede utilizar para apagar el sistema.

Herramientas de corrección

La funcionalidad Cyber Hygiene de IBM Intelligent Operations Center proporciona herramientas de corrección para corregir vulnerabilidades en el sistemaIBM Intelligent Operations Center instalado.

Las herramientas de corrección se ejecutan cuando se ejecuta Cyber Hygiene una vez completada la instalación deIBM Intelligent Operations Center. Estas herramientas también se pueden ejecutar cuando el sistema está en producción para encontrar y corregir vulnerabilidades que pudieran haber creado al instalar otros productos en los servidores o como resultado del uso del sistema.

Escáner de vulnerabilidades

El escáner consiste en scripts que revisan el sistema IBM Intelligent Operations Center e identifican vulnerabilidades. Por ejemplo, el escáner identifica directorios con privilegios de escritura para cualquier usuario.

El escáner crea un archivo de hallazgos utilizado por los scripts de corrección. El archivo de hallazgos indica las vulnerabilidades identificadas en el sistema IBM Intelligent Operations Center.

Los scripts del escáner no realizan cambios en el sistema IBM Intelligent Operations Center. El escáner solo identifica las vulnerabilidades. Se puede utilizar tras la corrección para validar los cambios realizados por los scripts de corrección.

Scripts de corrección de vulnerabilidades

Cyber Hygiene tiene tres tipos de scripts de corrección:

- Scripts que realizan cambios de configuración que no requieren exploración, pueden revertirse fácilmente o no tienen un impacto de tiempo de ejecución significativo en el sistema. Por ejemplo, cambiar el permiso de acceso al archivo predeterminado de las páginas del manual a 644.
- Un script para inhabilitar el inicio de sesión remoto con la cuenta `root`.
- Un script que procesa el archivo de hallazgos creado por el escáner y resuelve las vulnerabilidades identificadas.

  Debe prestar atención a la hora de utilizar el script una vez instalados productos adicionales. Algunos productos requieren una configuración menos estricta y pueden no funcionar correctamente tras la ejecución de estos scripts. Revise los archivos de hallazgos creados por los scripts del escáner en busca de riesgos potenciales antes de ejecutar cualquier script de corrección.

Registros de corrección

Los scripts de exploración y corrección registran sus acciones en cuatro archivos de registro en cada servidor de IBM Intelligent Operations Center. Estos registros se encuentran en el directorio `/var/BA15/CH/results`. Los subdirectorios contienen copias de trabajo de los resultados de la exploración y corrección.

El escáner se ejecuta dos veces: una para corregir las vulnerabilidades y otra para registrar las correcciones que no se han realizado. El registro de la segunda ejecución puede ser utilizado por el administrador para determinar si se deben implementar pasos de corrección manual.

Documentación de Cyber Hygiene

La documentación está disponible para ayudar al cliente a evaluar los cambios aplicados al sistema IBM Intelligent Operations Center instalado. Esta documentación ayuda con la certificación y acreditación de sistemas para su uso en producción.

La documentación incluye una descripción general de la estrategia global de Cyber Hygiene, el motivo por el cual se han implementado algunos valores predeterminados y una hoja de cálculo con el estado de las vulnerabilidades marcadas como DISA. Se puede utilizar la hoja de cálculo durante las evaluaciones de seguridad del producto.

Información relacionada:

 La implementación de Cyber Hygiene en IBM Intelligent Operations Center 1.5

Capítulo 4. Integración de la solución

Los productos y servicios se pueden integrar con los datos de incorporación de IBM Intelligent Operations Center relacionados con sucesos.

Los datos de sucesos comunicados a IBM Intelligent Operations Center pueden estar en Protocolo Común de Alertas o en otros protocolos.

Los sucesos pueden relacionarse con indicadores de rendimiento clave (KPI) supervisados por IBM Intelligent Operations Center. Los sucesos de IBM Intelligent Operations Center también se pueden relacionar con procedimientos de operación estándar y con los recursos disponibles. La solución proporciona un servicio de administración de informes, de manera que puede producir informes y resúmenes actualizados de los datos de sucesos.

Ejemplos de sistemas que se pueden integrar

Los productos y servicios se pueden integrar con IBM Intelligent Operations Center .

Ejemplos de sistemas y servicios incluyen:

- Sistemas que informan sobre problemas de seguridad públicos.
- Sistemas que informan sobre sucesos de tráfico.
- Sistemas que informan sobre el uso y la calidad del agua.
- Sistemas que proporcionan datos sobre paradas y estado de las órdenes de trabajo relacionadas.

Estos sistemas tienen que ser capaces de comunicarse conIBM Intelligent Operations Center y enviar sucesos y medidas de un protocolo soportado a la cola de sucesos de entrada de IBM Intelligent Operations Center .

Conceptos relacionados:

"Uso de la cola de sucesos de entrada definida por IBM Intelligent Operations Center" en la página 104
Se pueden publicar sucesos CAP en IBM Intelligent Operations Center dirigiéndolos a la instancia de WebSphere Message Broker incluida.

"Integración con el protocolo común de alertas" en la página 97
El Protocolo Común de Alertas (CAP) se utiliza para intercambiar información entre IBM Intelligent Operations Center y los sistemas externos.

Protocolos y puntos de integración

Se pueden integrar otros sistemas con la solución a través de los servicios y las políticas de IBM Intelligent Operations Center. Se pueden recibir datos en formato Common Alerting Protocol (CAP) y en otros protocolos.

Sucesos y KPI

sucesos de proceso de IBM Intelligent Operations Center e indicadores de rendimiento clave (KPI) para determinar cómo se muestra la información.

Se pueden integrar otros productos y servicios con IBM Intelligent Operations Center a través del servicio bus de mensajería. Los KPI se supervisan mediante el servicio de supervisión empresarial.

IBM Intelligent Operations Center recibe los sucesos. Estos sucesos se pueden mostrar en un portlet de Detalles y pueden afectar a lo que se muestra en los portlets del mapa.

La definición de KPI determina cómo se muestran los KPI en los portlets Estado y Obtención de detalles de indicador clave de rendimiento. La definición de KPI también puede determinar cómo se muestra la información sobre sucesos. Por ejemplo, si se sobrepasa un umbral de ICR, el suceso podría señalarse con una urgencia o gravedad más alta. Los sucesos sin las definiciones de KPI correspondientes se muestran según la información recibida sobre el suceso.

Para obtener más información sobre los KPI creados e integrados, consulte el enlace al final de este tema.

Conceptos relacionados:

"Creación e integración de KPI" en la página 113
Los modelos de KPI se pueden crear y modificar utilizando un kit de herramientas de desarrollo de supervisión de negocio y un portlet de gestión de KPI.

Política para las actualizaciones de KPI

La política de IBM Intelligent Operations Center determina si un suceso entrante es una actualización de suceso de KPI, después, lo envía a procesar para generar una actualización de KPI o una alerta dependiendo de los parámetros. El suceso de KPI lo determina<code>KPI</code> en el bloque de alerta de Protocolo Común de Alertas XML.

Si se confirma el suceso como actualización KPI, la política comprueba los parámetros KPI y genera un XML de sucesos KPI para enviarlo a IBM WebSphere Business Monitor para su procesamiento.

La tabla siguiente muestra una actualización de suceso KPI de ejemplo.

Tabla 29. Propiedades del suceso KPI de muestra

Propiedad	**Valor**
Remitente	security@rtp.city.gov
Tipo de suceso	Tiempo de respuesta del crimen
Estado del suceso	Real- Aplicable por todos los destinatarios objetivo
Alcance del suceso	Público - Para la difusión general a audiencias sin restricción
Categoría	Seguridad
Gravedad	Grave
Certeza	Probablemente
Urgencia	Inmediato
Tipo de mensaje	Alerta - Información inicial que requiere la atención de los destinatarios objetivo
Descripción	Robo
Fecha y hora de envío	2012-02-17T17:06:00+01:00
Fecha / hora inicio	2012-02-16T15:47:00+01:00
Fecha / hora respondido	2012-02-17T17:06:00+01:00

La tabla siguiente muestra los parámetros KPI de muestra asociados con la actualización de suceso KPI en Tabla 29.

Tabla 30. Parámetros de suceso KPI de muestra

Parámetro	**Valor**
Número del informe	1111
Distrito	Distrito uno
Respondido	2011-02-15T15:05:07-05:00

Conceptos relacionados:

"Estado" en la página 297
Utilice el portlet Estado para ver el estado de los indicadores clave de rendimiento (ICR) para una única organización o en varias organizaciones.

"Notificaciones" en la página 293
Utilice el portlet Notificaciones para ver sus mensajes de alerta y sus detalles.

Integración con el protocolo común de alertas

El Protocolo Común de Alertas (CAP) se utiliza para intercambiar información entre IBM Intelligent Operations Center y los sistemas externos.

El CAP es un formato genérico para intercambiar alertas de emergencia y avisos públicos en varias redes. Esto proporciona un formato de mensaje principal abierto y no propietario para todos los tipos de alertas y notificaciones. El CAP es compatible con técnicas emergente como los servicios web, mientras ofrece prestaciones mejorada. Estas prestaciones incluyen:

- Destino geográfico flexible utilizando formas de latitud y longitud y otras representaciones geoespaciales en tres dimensiones
- Mensajería multilíngüe y de múltiple audiencia
- Vencimientos y horas efectivas retrasadas y graduales
- Funciones de cancelación y actualización de mensajes mejoradas
- Soporte de plantilla para la formulación de mensajes de aviso efectivos y completos
- Cifrado digital y compatibilidad de firmas
- Imágenes digitales y recursos de audio

Los sucesos son mensajes de datos autocontenidos que pueden enviar o consumir todos los componentes. Los sucesos se pueden publicar en colas de temas y los puede leer todos los interesados potencialmente en suscribir sistemas IT. El CAP ayuda a estandarizar el contenido del suceso para que varios dominios puedan enviar y recibir sucesos en un formato común utilizando convenciones comunes. El estándar define los campos opcionales y obligatorios en el registro de sucesos y los valores aceptables para esos campos. La gestión del procesamiento de sucesos puede mediar entre formatos de legado y el formato estandarizado. El CAP se puede ampliar para gestionar operaciones del día a día además de las situaciones de emergencia.

Mínimamente, los sucesos tienen que tener:

- Un identificador de suceso exclusivo que contenga:
  - El remitente (sistema o humano)
  - La organización que envía el suceso
  - Número de serie en el sistema que envía
  - Indicación de fecha y hora de la creación del suceso
- Información que permite a los destinatarios definir y priorizar respuestas:
  - Urgencia – la rapidez con la que los destinatarios deben responder a la alerta
  - El nivel de amenaza para la vida y propiedad
  - Certeza – un rango de probabilidad desde el 100%, se ha observado el proceso, al 0%, no se espera que el suceso ocurra ahora
  - Hora prevista para sucesos que pueden producirse en el futuro
  - Duración de los sucesos que se han informado anteriormente y de cuya continuación se está informando
  - Duración anticipada de sucesos que representan una situación que no se puede corregir inmediatamente
  - Directivas y acciones impuestas y recomendadas

- Información para permitir que el suceso se correlacione:
  - Referencias del modelo semántico de ciudad (si existe uno)
  - Coordenadas geoespaciales
  - Referencia a un suceso de requisito previo o a un suceso que fue la causa precipitante
  - Identificado de activo exclusivo para cualquier implicado
- Descripciones textuales legibles para el humano:
  - Descripción de ubicación
  - Descripción de la actividad

El uso de CAP ayuda a minimizar el intercambio de datos por suceso. Dado que los sucesos están formateados en XML, el formato de datos lo pueden escribir y leer varios sistemas, por lo tanto, si se impide el intercambio de datos o de datos sin sentido se crea una confusión peligrosa.

El IBM Intelligent Operations Center proporciona un almacén persistente de alertas CAP y una interfaz estándar para presentarlos.

Aunque IBM Intelligent Operations Center acepta toda la estructura del CAP, IBM Intelligent Operations Center solo utiliza algunos datos al calcular los indicadores clave de rendimiento (KPI).

El IBM Intelligent Operations Center utiliza WebSphere Message Broker para integrar sucesos utilizando el CAP.

El IBM Intelligent Operations Center soporta OASIS Protocolo Común de Alertas versión 1.2.

Conceptos relacionados:

"Utilización del PAC para sucesos de ICR" en la página 100
El WebSphere Message Broker, que se proporciona como parte de IBM Intelligent Operations Center, acepta mensajes de suceso CAP y utiliza los datos en los cálculos del indicador clave de rendimiento (KPI) .

"Uso de CAP para sucesos distintos a KPI" en la página 103
También puede usar datos CAP para proporcionar datos sobre sucesos no asociados con cálculos KPI.

Información relacionada:

OASIS Common Alerting Protocol versión 1.2

Estructura CAP

Cada mensaje de alerta CAP consta de un segmento de <alerta> que puede contener uno o más segmentos de <información> . Cada segmento de <información> puede incluir uno o más segmentos de <área> . En la mayoría de casos, los mensajes CAP con un <msgType> con un valor de *alerta* incluye al menos un elemento <info>.

A continuación están los elementos de mensaje principales.

- <alert>

  El segmento <alert> proporciona información básica sobre el mensaje actual: su propósito, su fuente, y su estado. También tiene un identificador exclusivo para el mensaje y se vincula con otros mensajes relacionados. Un segmento <alert> se puede utilizar solo para el reconocimiento de los mensajes, cancelaciones u otras funciones del sistema; sin embargo, la mayoría de los segmentos de alerta incluyen al menos un segmento <info> .
- <info>

  El segmento <info> determina un suceso real o anticipado en términos de urgencia (el tiempo disponible para preparar), gravedad (la intensidad del impacto) y la certeza (confianza en la observación y predicción). También proporciona descripciones textuales y categóricas del suceso del asunto. El segmento <info> también puede proporcionar instrucciones para respuestas adecuadas por

parte de los destinatario del mensaje y otros detalles, por ejemplo, la duración del peligro, parámetros técnicos, información del contacto y enlaces a fuentes de información adicionales. Se pueden utilizar varios segmentos <info> para describir parámetros diferentes, como bandas de intensidad o probabilidad diferentes, o para proporcionar información en varios idiomas.

- <resource>

  El segmento <resource> proporciona una referencia opcional a la información adicional relacionada con el segmento <info> . Puede hacer referencia a un activo digital como una imagen o un archivo de audio.

- <area>

  El segmento <area> describe un área geográfica a la que se aplica el segmento <info> . Se admiten descripciones codificadas y textuales (como códigos postales), pero las representaciones preferidas utilizan formas geoespaciales, polígonos y círculos, y una altitud o rango de altitud expresada en términos de latitud, longitud y altitud estándar, de acuerdo con los datos geoespaciales especificados.

Conceptos relacionados:

"Utilización del PAC para sucesos de ICR" en la página 100
El WebSphere Message Broker, que se proporciona como parte de IBM Intelligent Operations Center, acepta mensajes de suceso CAP y utiliza los datos en los cálculos del indicador clave de rendimiento (KPI) .

"Uso de CAP para sucesos distintos a KPI" en la página 103
También puede usar datos CAP para proporcionar datos sobre sucesos no asociados con cálculos KPI.

Tipos de sucesos

IBM Intelligent Operations Center admite varios tipos de sucesos CAP.

Suceso real/previsto

Los mensajes de sucesos reales/previstos son mensajes no solicitados enviados por varios dominios sobre condiciones anormales o excepciones. Estos mensajes también cubren violaciones del indicador clave de rendimiento (KPI) donde se creó un suceso.

Confirmación

Una confirmación es un mensaje con los siguientes valores de campo en el elemento <alert> :

- El valor <msgType> está establecido en **ACK** lo que significa que el remitente reconoce la recepción y aceptación de mensajes identificados en <references>.
- El campo <references> contiene los identificadores de mensajes ampliados (en formato sender, identifier, sent) de un mensaje o mensajes CAP anteriores a los que se hace referencia por el reconocimiento.
-

  Nota: El elemento <info> es opcional para una confirmación.

Respuesta

Una respuesta es un mensaje CAP con los siguientes valores de campo en el elemento <alert> :

- El valor <msgType> es **Alerta**.
- El valor <note> es **Respuesta**.
- El elemento <references> debe contener los identificadores del mensaje CAP para los que esto es una respuesta.

Por ejemplo, cuando un operador de ciudad envía un **Consejo sobre apagón de la ciudad** a varios dominios, estos dominios devuelven una repuesta al consejo después de realizar un análisis de impacto en sus funciones individuales.

Incidencia

Las incidencias se utilizan para intercalar varios mensajes que hacen referencia a diferentes aspectos de la misma incidencia. Los mensajes CAP de incidencia actúan como contenedor de todos los sucesos relacionados con una incidencia específica. Estos sucesos pueden estar en dominios diferentes.

Un consejo puede ascender a incidencia cuando los dominios devuelven respuestas al consejo indicando que varios dominios impactan al requerir una acción coordinada. El elemento <incident> que está en todos los sucesos relacionados se llena con el valor <identifier> del suceso de la incidencia. Los sucesos relacionados son sucesos donde el valor<references> es el mismo que el valor <identifier> del suceso de la incidencia.

Una incidencia es un mensaje CAP con los siguientes valores de campo en el elemento <alert>:

- El valor <msgType> es **Alerta**.
- El valor <note> es **Incidencia**.
- El elemento <references> debe contener los identificadores del mensaje CAP que es padre (la causa raíz) de este suceso.
- El elemento <incidents> debe contener su propio identificador

Actualizar

Una actualización es un mensaje CAP con los siguientes valores de campo en el elemento <alert>:

- El elemento <msgType> se establece en **actualización** que significa que esta actualización reemplaza los mensajes anteriores identificados en el elemento <references> .
- El elemento <references> contiene los identificadores de mensajes ampliados (en formato sender, identifier, sent) de un mensaje o mensajes CAP anteriores a los que hace referencia la actualización.

Cancelar

Una cancelación es un mensaje CAP con los siguientes valores de campo en el elemento <alert> :

- El elemento <msgType> se establece en **Cancelar** lo que significa que este mensaje cancela los mensajes anteriores identificados en el elemento <references> .
- El elemento <references> contiene los identificadores de mensajes ampliados (en formato sender, identifier, sent) de un mensaje o mensajes CAP anteriores a los que hace referencia esta cancelación.
- El elemento <note> contiene una explicación de porqué o cómo se borra esta alerta.

Información relacionada:

OASIS Common Alerting Protocol versión 1.2

Utilización del PAC para sucesos de ICR

El WebSphere Message Broker, que se proporciona como parte de IBM Intelligent Operations Center, acepta mensajes de suceso CAP y utiliza los datos en los cálculos del indicador clave de rendimiento (KPI) .

Tabla 31 lista los elementos de datos utilizados en cálculos de KPI:

Tabla 31. Elementos CAP utilizados en cálculos de KPI de IBM Intelligent Operations Center KPI

Obligatorio u opcional	Elemento de datos (normativa)	Descripción
Necesario	Message_ID (identificador)	Identificador de mensaje único
Necesario	Sender_ID (remitente)	Identificador de remitente exclusivo

Tabla 31. Elementos CAP utilizados en cálculos de KPI de IBM Intelligent Operations Center KPI (continuación)

Obligatorio u opcional	Elemento de datos (normativa)	Descripción
Necesario	`SentDateTime` (enviado)	Fecha y hora en que se envió el mensaje. Por ejemplo: `2011-02-07T 16:49:00-05:00` contiene la fecha y la hora en que se envió un mensaje. Los últimos seis caracteres indican la zona horaria del suceso CAP, en relación con la hora de Greenwich (GMT). En este caso, el suceso se produjo a las 16:49:00, GMT menos 5 horas, es decir, hora estándar del este (EST). Este código significa que cuando se muestra el suceso, se convierte de EST a la zona horaria del usuario. En cambio, si desea codificar los sucesos CAP en GMT, cambie el sufijo a -00:00 como en este ejemplo: `2011-02-07T 16:49:00-00:00`.
Necesario	`MessageStatus` (estado)	Estado del mensaje, puede ser una de las opciones siguientes: • `Real` • `Ejercicio` • `Sistema` • `Prueba` • `Borrador`
Necesario	`MessageType` (msgType)	Tipo de mensaje, puede ser una de las opciones siguientes: • `Alertar` • `Actualizar` • `Cancelar` • `Ack` • `Error`
Opcional	`Source` (origen)	Origen del mensaje
Necesario	`Scope` (alcance)	Contiene el valor `Public`
Necesario	`Code` (código)	Contiene el valor `KPI` para ocultar este suceso de la lista de portlets de Sucesos.
Necesario	`EventCategory` (categoría)	Uno de los siguientes: • `País` • `Cumplido` • `Seguridad` • `Seguridad` • `Rescate` • `Incendio` • `Salud` • `Ent.` • `Transporte` • `Infra` • `CBRNE` • `Otros`
Necesario	`EventType` (suceso)	Descripción del suceso o KPI. Por ejemplo: `Police_Department_Budget`

Tabla 31. Elementos CAP utilizados en cálculos de KPI de IBM Intelligent Operations Center KPI (continuación)

Obligatorio u opcional	Elemento de datos (normativa)	Descripción
Necesario	`Urgency` (urgencia)	Uno de los siguientes: • `Inmediato` • `Esperado` • `Futuro` • `Anterior` • `Desconocido`
Necesario	`Severity` (gravedad)	La gravedad se indica mediante una de las opciones siguientes: • `Extremo` • `Severo` • `Moderado` • `Menor` • `Desconocido`
Necesario	`Certainty` (certeza)	La gravedad se indica mediante una de las opciones siguientes: • `Observado` • `Probable` • `Posible` • `Poco probable` • `Desconocido`
Opcional	`EventCode` (eventCode)	Pares nombre-valor para tipo de suceso.
Opcional	`OnsetDateType` (comienzo)	Fecha y hora en que comienza el suceso Por ejemplo: `2011-02-08T16:49:00-05:00`
Opcional	`SenderName` (senderName)	Nombre de la entidad que ha iniciado la alerta. Por ejemplo: `Police Department`
Opcional	`EventDescription` (descripción)	Descripción detallada del suceso o KPI
Opcional	`Parameter` (parámetro)	Datos adicionales asociados con el suceso o KPI.
Opcional	`AreaGeocode` (geocode)	Campo que se puede utilizar para proporcionar información cuando el KPI es dependiente de la ubicación

Para obtener más información, consulte el enlace relacionado al final del tema en la especificación Protocolo Común de Alertas OASIS.

El código siguiente es el ejemplo de un suceso que comunica un accidente de tráfico.

```
<?xml version="1.0" encoding="UTF-8"?>
<cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.2"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:oasis:names:tc:emergency:cap:1.2 CAP-v1.2-os.xsd ">
 <cap:identifier>1112</cap:identifier>
 <cap:sender>Transportation</cap:sender>
 <cap:sent>2011-02-17T15:00:00-05:00</cap:sent>
 <cap:status>Actual</cap:status>
 <cap:msgType>Alert</cap:msgType>
 <cap:scope>Public</cap:scope>
 <cap:code>KPI</cap:code>
 <cap:info>
```

```
  <cap:category>Transport</cap:category>
  <cap:event>Traffic_Accident</cap:event>
  <cap:urgency>Unknown</cap:urgency>
  <cap:severity>Extreme</cap:severity>
  <cap:certainty>Unknown</cap:certainty>
  <cap:eventCode>
   <cap:valueName>OwningOrg</cap:valueName>
   <cap:value>Police</cap:value>
  </cap:eventCode>
  <cap:onset>2011-02-17T15:00:00-05:00</cap:onset>
  <cap:senderName>Transportation</cap:senderName>
  <cap:description>Single car crash</cap:description>
  <cap:parameter>
   <cap:valueName>accident number</cap:valueName>
   <cap:value>1112</cap:value>
  </cap:parameter>
 </cap:info>
</cap:alert>
```

Conceptos relacionados:

"Ubicación de la interfaz de usuario" en la página 145
Los valores de navegador determinan el idioma y los valores de fecha y hora para la interfaz de usuario de IBM Intelligent Operations Center . Un administrador puede personalizar los formatos de fecha y hora.

"Problemas conocidos y soluciones" en la página 336
Esta sección contiene una lista de los problemas que se producen con más frecuencia y una solución para cada elemento.

Información relacionada:

OASIS Common Alerting Protocol versión 1.2

Uso de CAP para sucesos distintos a KPI

También puede usar datos CAP para proporcionar datos sobre sucesos no asociados con cálculos KPI.

Los datos CAP recibidos por IBM Intelligent Operations Center que no están asociados con los KPI definidos se añaden a los portlets de Sucesos y Mapa en IBM Intelligent Operations Center.

El código siguiente es un ejemplo de suceso no de KPI. Tenga en cuenta que para los sucesos de KPI, debe establecer el valor de la etiqueta `code` en `Event`.

```
<p>
 <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
   <identifier>f30f190c-41fd-431e-ace9-88b725f1a3fc</identifier>
   <sender>TestGenerator</sender>
   <sent>2012-03-26T15:47:24-00:00</sent>
   <status>Actual</status>
   <msgType>Alert</msgType>
   <scope>Public</scope>
   <restriction/>
   <code>Event</code>
   <info>
     <language>en_US</language>
     <category>Infra</category>
     <event>Water Main Break</event>
     <urgency>Immediate</urgency>
     <severity>Moderate</severity>
     <certainty>Observed</certainty>
     <headline>Major water line leak at NW 20th St.</headline>
     <description>Leak is located at the intersection of NW 20th Street and NW 9th Avenue.
     Street flooding starting tooccur. Immediate action required.</description>
     <area>
       <circle>25.79518,-80.21110 0</circle>
```

```
    </area>
   </info>
 </alert>
</p>
```

Uso de la cola de sucesos de entrada definida por IBM Intelligent Operations Center

Se pueden publicar sucesos CAP en IBM Intelligent Operations Center dirigiéndolos a la instancia de WebSphere Message Broker incluida.

Se puede configurar la publicación de clientes para señalar directamente a la cola de entrada de sucesos CAP de WebSphere Message Broker , o pueden utilizar los recursos JMS de WebSphere Application Server definidos en servidor del portal . Estos recursos JMS apuntan a la cola de WebSphere Message Broker que recibe sucesos de CAP. Se crean los siguientes recursos JMS cuandoIBM Intelligent Operations Center está instalado:

- Fábrica de conexión de cola
  - Nombre: `ioc.mb.con.factory`
  - Nombre de JNDI: `jms/ioc.mb.con.factory`
- Cola
  - Nombre: `ioc.cap.in.q`
  - Nombre de JNDI: `jms/ioc.cap.in.q`

Conceptos relacionados:

"Comunicación de sucesos de KPI entre IBM WebSphere Business Monitor y IBM Intelligent Operations Center" en la página 120
IBM WebSphere Business Monitor puede enviar sucesos salientes desde un contexto de KPI o de supervisión a IBM Intelligent Operations Center.

Creación de sucesos utilizando el servicio de publicación

Puede enviar sucesos a IBM Intelligent Operations Center a través de los servicios web a un servicio de publicación.

Puede crear aplicaciones cliente que se pueden integrar en una instancia desplegada de IBM Intelligent Operations Center. Puede utilizar una aplicación cliente para pasar alertas CAP desde una aplicación cliente de terceros a IBM Intelligent Operations Center llamando a los métodos expuestos por la clase de programa de utilidad de servicios de aplicación de publicación y el servlet IBM Intelligent Operations Center Publisher.

Desarrollo con clases de programa de utilidad comunes

Si desea crear una aplicación cliente que llame al servicio de aplicación de publicación, antes de comenzar debe establecer las clases de programa de utilidad comunes. Después de finalizar el desarrollo de la aplicación cliente, expórtela como archivo WAR que después importa a WebSphere Application Server.

Acerca de esta tarea

Utilice el siguiente procedimiento si desea desarrollar una aplicación cliente con las clases de programa de utilidad comunes:

- Antes de desarrollar la aplicación cliente, añada los archivos JAR `iss_common` y `icu4j-4_4_2` a la vía de acceso de compilación del proyecto. Se necesitan los archivos JAR durante el tiempo de compilación.
- Después de desarrollar la aplicación cliente, expórtela como archivo WAR.
- Importe el archivo WAR en WebSphere Application Server y configúrelo para hacer referencia a las bibliotecas compartidas.

Procedimiento

1. Ubique el archivo `iss_common.jar` y el archivo `icu4j-4_8_1_1.jar` en el directorio de instalación IBM Intelligent Operations Center, `/opt/IBM/iss/common/lib`.
2. Copie el archivo `iss_common.jar` y el archivo `icu4j-4_8_1_1.jar` en una ubicación de su equipo de desarrollo.
3. Para añadir archivos JAR a la vía de acceso de compilación del proyecto, en IBM Intelligent Operations Center API, siga los subpasos siguientes para `iss_common.jar` y `icu4j-4_8_1_1.jar`:
   a. Haga doble clic en **Proyectos de portlet**.
   b. Pulse **Vía de acceso de compilación** > **Configurar vía de acceso de compilación**.
   c. Pulse la pestaña **Bibliotecas** y pulse **Añadir JAR externos...**.
   d. Navegue al directorio que contiene el archivo JAR.
   e. Pulse el archivo JAR y, a continuación, pulse **Abrir**.
4. Cuando haya terminado de desarrollar la aplicación cliente, expórtela como archivo WAR.
5. En la consola administrativa de WebSphere Application Server , utilice el asistente de importación para importar el archivo WAR de la aplicación cliente.
6. Para configurar el archivo WAR para que haga referencia a las referencias de bibliotecas compartidas, lleve a cabo los subpasos siguientes:
   a. En la consola administrativa de WebSphere Application Server , seleccione la casilla de verificación al lado del archivo WAR importado, a continuación, pulse **Actualizar**.
   b. Pulse **Referencias de bibliotecas compartidas**.
   c. En la ventana Referencias de bibliotecas compartidas , seleccione la casilla de verificación **Aplicación** .
   d. Pulse **Bibliotecas compartidas de referencia**.
   e. Mueva **ISSCommonJars** y **IOCCommonJars** desde la lista Disponible a la lista Seleccionada y, a continuación, pulse **Aceptar**.
   f. Para guardar los cambios, pulse **Aceptar**.

Utilización del servicio de aplicación de publicación

La herramienta de inyector de suceso de servicio de publicación se proporciona como programa de utilidad de Java. Puede crear una aplicación cliente que pasa el XML de CAP a IBM Intelligent Operations Center llamando a los métodos expuestos por el servicio de aplicación de publicación. También puede pasar notificaciones.

El servicio de publicación es una clase de programa de utilidad del proyecto `iss_common_utils`, que se genera en el archivo `iss_common.jar`. El servicio de aplicación de publicación expone los métodos estáticos `publishEvent` y `publishNotification`. Antes de crear aplicaciones cliente para el servicio de aplicación de publicación, debe establecer las clases del programa de utilidad comunes. Para obtener más información, consulte el enlace al final del tema.

Para asegurarse de que el código utilizado para llamar al servicio de publicación tiene acceso a las configuraciones de cola JMS correctas, debe desplegarlo en servidor de aplicaciones.

El siguiente código de ejemplo muestra cómo llamar al servicio de aplicación de publicación:

```
import com.ibm.iss.common.publisher.Publisher;

String capMessage = request.getParameter(EVENT_TEXT_KEY);

int status = Publisher.publishEvent(capMessage);

si (status == Publisher.STATUS_SUCCESS) {
logger.traceFine(este, methodName, "Event submit request was performed successfully");
}
además si (status == Publisher.STATUS_EXCEPTION_NAMING) {
logger.traceFine(este, methodName, "Error sending CAP Event Message. Requiere definir los recursos JMS.");
```

```
}
además si (status == Publisher.STATUS_EXCEPTION_JMS) {
logger.traceFine(este, methodName, "Error sending CAP Event Message. Falló la conexión a los recursos JMS.");
}
además { //Other error code
logger.traceFine(este, methodName, "Error sending CAP Event Message. Returned status = " + status);
}
```

Si utiliza el portlet Ejemplo de aplicación de publicación , no es necesario crear el código para llamar al servicio de aplicación de publicación o grabar mensajes CAP.

Conceptos relacionados:

"Ejemplo de aplicación de publicación" en la página 107
Utilice el portlet Ejemplo de aplicación de publicación para publicar sucesos de Common Alerting Protocol (CAP) en IBM Intelligent Operations Center.

Tareas relacionadas:

"Desarrollo con clases de programa de utilidad comunes" en la página 104
Si desea crear una aplicación cliente que llame al servicio de aplicación de publicación, antes de comenzar debe establecer las clases de programa de utilidad comunes. Después de finalizar el desarrollo de la aplicación cliente, expórtela como archivo WAR que después importa a WebSphere Application Server.

Uso del servlet de aplicación de publicación

El servlet de aplicación de publicación acepta los parámetros de la solicitud POST para publicar el XML de CAP, crear nuevos sucesos o crear sucesos modificados a partir de sucesos o incidencias existentes.

Envío de solicitudes POST al servlet de aplicación de publicación

El servlet de aplicación de publicación llama al servicio de aplicación de publicación para poner el XML de CAP en las colas que se introducen en IBM Intelligent Operations Center. El servlet de aplicación de publicación está ubicado en `/ibm/iss/common/rest/publisher`. La tabla siguiente muestra cómo enviar solicitudes POST al servlet de aplicación de publicación.

Tabla 32. Solicitudes POST del servlet de aplicación de publicación

Tipo de suceso que se va a publicar	Código de solicitud POST
Publicar un nuevo suceso CAP	`action=publishEvent&source=xml&xml=`*`CAP_event_XML`*
Modificar un suceso existente	`action=publishEvent&source=existing&id=`*`event_id`*
Publicar un nuevo suceso en blanco	`action=publishEvent&source=new`

Parámetros opcionales

Puede aplicar parámetros opcionales a cada una de las opciones de publicación adjuntando el código siguiente a la solicitud POST: `&`*`parameter_name=new_value`*

Los siguientes parámetros opcionales están disponibles.

- areaDesc
- categoría
- certeza
- código
- contacto
- descripción
- suceso
- título
- latitud

- longitud
- msgType
- aleatorizar
- aleatorizado
- randomizeArea
- randomizeTime
- remitente
- senderName
- gravedad
- estado
- urgencia

Por ejemplo, para publicar un nuevo suceso en blanco y, después, establecer el titular para `Traffic`, el código de solicitud POST es: `servletURL&action=publishEvent&source=new&headline=Traffic Accident`

Creación y publicación de sucesos de prueba

El IBM Intelligent Operations Center proporciona el portlet Ejemplo de aplicación de publicación y e l portlet Script de suceso para la creación y publicación de sucesos de prueba.

Conceptos relacionados:

"Creación de sucesos utilizando el servicio de publicación" en la página 104
Puede enviar sucesos a IBM Intelligent Operations Center a través de los servicios web a un servicio de publicación.

Ejemplo de aplicación de publicación

Utilice el portlet Ejemplo de aplicación de publicación para publicar sucesos de Common Alerting Protocol (CAP) en IBM Intelligent Operations Center.

El portlet Ejemplo de aplicación de publicación es una herramienta de pruebas automatizada diseñada para la gestión del administrador o la verificación de una solución. Un administrador puede utilizar el portletEjemplo de aplicación de publicación como aplicación cliente para probar la publicación de mensajes CAP en IBM Intelligent Operations Center. El portlet Ejemplo de aplicación de publicación puede eliminar el requisito para crear manualmente una aplicación cliente de prueba.

Creación de sucesos y notificaciones

Para iniciar el portlet Ejemplo de aplicación de publicación, en la interfaz de administración de WebSphere Portal haga clic en **Intelligent Operations** > **Herramientas de demostración** > **Aplicación de publicación de sucesos de muestra**.

En la pestaña **CAP de suceso** del portlet Ejemplo de aplicación de publicación , puede completar un formulario para diseñar sucesos con XML. Emita el formulario para activar el flujo de sucesos CAP de muestra en el sistema.

El portlet Ejemplo de aplicación de publicación también contiene una pestaña **Formulario de suceso** para la creación de nuevos sucesos cuando no es necesario editar el XML. Complete el formulario en la pestaña **Formulario de sucesos** para enviar los detalles del suceso de CAP. Si desea crear nuevos sucesos con propiedades basadas en las propiedades de un suceso existente, escriba el ID de alerta CAP correspondiente al suceso existente en el campo **ID**.

El portlet Ejemplo de aplicación de publicación contiene una pestaña **Notificación** para probar el subsistema de notificaciones de IBM Intelligent Operations Center. En la pestaña **Notificaciones** , puede

completar un formulario para emitir una notificación de alerta para un grupo específico. Los valores que entra en el campo **Enviado a grupos** debe coincidir con grupos de usuarios existentes, por ejemplo, CityWideOperator, CityWideExecutive, porque sólo se muestran las alertas coincidentes en la lista del portlet Notificaciones .

Valores aleatorios

En las pestañas **CAP de suceso** y **Formulario de suceso** , si selecciona la casilla de verificación **Aleatorizar suceso** , el portlet alerta automáticamente a las propiedades de los sucesos que publica de la siguiente manera:

- **ID**: el portlet genera una cadena de ID exclusivo para cada suceso, porque los ID de suceso deben ser exclusivos en IBM Intelligent Operations Center.
- **Indicación de fecha y hora**: El portlet aumenta el valor de la indicación de fecha y hora para cada suceso enviado para que cada suceso de la secuencia llegue a una hora diferente.
- **Ubicación**: El portlet aleatoriza la latitud y longitud para cada suceso, dentro de un rango, para que cumplan con el formato requerido para latitud, longitud y radio; por ejemplo, `32.9525,-115.5527 5`. El valor del radio no se cambia.

Personalización del portlet Ejemplo de aplicación de publicación

Puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Referencia relacionada:

"Valores del portlet Ejemplo de aplicación de publicación" en la página 167
Personalice el portlet Ejemplo de aplicación de publicación cambiando los valores en los campos de la ventana **Valores compartidos** .

Creación de sucesos de muestra con XML

En la pestaña **CAP de suceso** , puede seleccionar una plantilla de suceso de CAP de muestra que puede utilizar para visualizar, modificar y publicar sucesos.

Antes de empezar

Inicialmente, seleccione una categoría de suceso. Las categorías representan las áreas primarias en las que se dividen los sucesos.

Tabla 33. Categorías de sucesos

Categoría	Descripción
CBRNE	Amenaza o ataque químico, biológico, radiológico, nuclear o explosivos de alto rendimiento
Medio ambiente	Contaminación y otro suceso medioambiental
Incendio	Extinción de incendios y rescate
Geofísico	Suceso geofísico, incluyendo deslizamiento de tierra
Salud	Suceso médico y de salud pública
Infraestructura	Utilidad, telecomunicación u otro suceso de infraestructura que no es transporte
Meteorológico	Suceso meteorológico, incluyendo inundaciones
Rescate	Rescate y recuperación
Seguridad	Emergencia general y seguridad pública
Seguridad	Seguridad local y privada, nacional, militar y cumplimiento de la ley
Transporte	Transporte público y privado

Tabla 33. Categorías de sucesos (continuación)

Categoría	Descripción
Otros	Otros sucesos

Acerca de esta tarea

Para obtener más información sobre las propiedades de los sucesos, siga el enlace situado al final de este tema, que le llevará al tema por portles de Detalles.

Procedimiento

1. En la interfaz de administración de WebSphere Portal, pulse **Intelligent Operations** > **Herramientas de demostración** > **Aplicación de publicación de sucesos de muestra**.
2. Pulse la pestaña **Suceso PAC**.
3. En la lista **Categoría**, seleccione una categoría de suceso.
4. Para el campo **Mensaje de suceso**, elija una de las siguientes opciones:
   - Para insertar el XML para el correspondiente mensaje CAP escrito previamente automáticamente en el campo **Mensaje del suceso** , de la lista **Suceso de muestra** , seleccione un suceso. Si lo desea, edite el XML para que se ajuste a sus necesidades.
   - En el campo **Mensaje de suceso**, especifique manualmente el XML para el mensaje de PAC desde cero.
5. En el campo **Recuento de instancias de suceso**, especifique el número de mensajes necesarios o bien utilice las flechas para seleccionar el número de mensajes necesarios. Puede enviar un único mensaje de PAC o una secuencia automatizada de mensajes.
6. Opcional: Marque el recuadro de selección **Selección aleatoria de sucesos**. Si selecciona **Selección aleatoria de sucesos**, se publica una secuencia de mensajes de PAC con los ID aleatorios aplicados. Los mensajes se publican a intervalos de tiempo incrementales y en ubicaciones aleatorias dentro de un rango.
7. Pulse **Enviar suceso**.

Resultados

El Ejemplo de aplicación de publicación llena IBM Intelligent Operations Center con sucesos y puede desencadenar ICR.

Conceptos relacionados:

"Detalles" en la página 278
Utilice el portlet Detalles para visualizar, supervisar y gestionar sucesos en IBM Intelligent Operations Center.

Creación de nuevos sucesos CAP o actualización de sucesos existentes sin XML

En la pestaña **Formulario de suceso** , puede completar un formulario para crear nuevos sucesos CAP o actualizar sucesos existentes, sin utilizar XML.

Acerca de esta tarea

Puede utilizar el formulario para crear un nuevo suceso o un suceso basado en valores de un suceso existente. Cuando crea un suceso basado en un suceso existente, ve el ID de alerta de CAP para hacer referencia al suceso existente. Cualquier valor que entre en el formulario sobrescribe los valores heredados desde el suceso CAP existente.Para obtener más información sobre las propiedades de los sucesos, siga el enlace situado al final de este tema, que le llevará al tema por portles de Detalles.

Procedimiento

1. En la interfaz de administración de WebSphere Portal, pulse **Intelligent Operations** > **Herramientas de demostración** > **Aplicación de publicación de sucesos de muestra**.
2. Pulse la pestaña **Formulario de sucesos**.
3. Para especificar un origen para el suceso, al lado de Origen pulse una de las siguientes opciones:
   - Para crear un suceso nuevo con valores basados en los valores que entra en el formulario, pulse **Nuevo**.
   - Para crear un suceso con valores basados en un suceso existente en la tabla de sucesos de CAP y utilizando un ID de alerta de CAP, pulse **Existente**.
4. En el campo **ID**, introduzca un ID en función de si va a crear un nuevo suceso, o un suceso basado en un ID de alerta CAP:
   - Si está creando un suceso nuevo, opcionalmente, entre un valor para **ID**. Si no entra un valor, se genera un identificador exclusivo.
   - Si está creando un suceso basado en un valor de ID de alerta de CAP, entre ese valor para **ID**. Cualquier valor que entre en el formulario sobrescribe los valores heredados desde el suceso CAP existente.
5. Si está creando un suceso nuevo, en el campo **Tipo de suceso** , entre uno de los siguientes tipos de suceso:

   Alertar
   Un suceso nuevo.

   Actualizar
   Una actualización para un suceso creado anteriormente.

   Cancelación
   Una cancelación de un suceso creado anteriormente.
6. En el campo **Titular** , entre un titular.
7. En la lista **Tipo de mensaje**, seleccione un tipo de mensaje.
8. Si está creando un suceso nuevo, en la lista **Código de suceso** , seleccione **Suceso** o **Incidencia**. Una incidencia tiene una importancia mayor que un suceso.
9. En la lista **Categoría** , seleccione una categoría.
10. En la lista **Urgencia** , seleccione una urgencia.
11. En la lista **Gravedad** , seleccione una gravedad.
12. En la lista **Certeza** , seleccione una certeza.
13. En el campo **Descripción**, especifique información adicional.
14. En el campo **Remitente** , entre una descripción del remitente del suceso.
15. En el campo **Recuento de instancia de suceso** , seleccione el número de mensajes requeridos. Puede enviar un único mensaje de PAC o una secuencia automatizada de mensajes.
16. Opcional: Marque el recuadro de selección **Selección aleatoria de sucesos**. Si selecciona **Selección aleatoria de sucesos**, se publica una secuencia de mensajes de PAC con los ID aleatorios aplicados. Los mensajes se publican a intervalos de tiempo incrementales y en ubicaciones aleatorias dentro de un rango.
17. Pulse **Enviar suceso**.

Conceptos relacionados:

"Detalles" en la página 278
Utilice el portlet Detalles para visualizar, supervisar y gestionar sucesos en IBM Intelligent Operations Center.

Notificaciones de prueba

Utilice la pestaña **Notificaciones** para crear notificaciones de prueba para probar el subsistema de notificaciones en IBM Intelligent Operations Center.

Acerca de esta tarea

En la pestaña **Notificación** , complete el formulario para enviar una alerta para grupos específicos. Para un usuario concreto, se muestra un mensaje de notificación de alerta en el portletNotificaciones sólo si el usuario es miembro de uno de los grupos Enviado a grupos especificado en las notificaciones.

Procedimiento

1. En la interfaz de administración de WebSphere Portal, pulse **Intelligent Operations** > **Herramientas de demostración** > **Aplicación de publicación de sucesos de muestra**.
2. Haga clic en la ficha **Notificación**.
3. Para crear una alerta, desde la lista **Tipo** , seleccione `Alerta` .
4. Opcional: En la lista **Categoría** , seleccione una categoría.
5. Opcional: En el campo **Titular** , entre un titular.
6. Opcional: En el campo **Descripción**, especifique información adicional.
7. Opcional: En el campo **Remitente** , entre una descripción del remitente del suceso.
8. Opcional: En el campo **Enviado a grupos** , entre una lista de grupos separada por punto y coma a la que enviar la alerta, por ejemplo, `;CityWideOperator;CityWideExecutive;`.

   Nota: Además de insertar un punto y coma entre cada nombre de grupo, asegúrese de que inserta un punto y coma al comienzo y al final de la lista.
   Una vez publicada, esta notificación de alerta se visualiza en el portlet Notificaciones únicamente por los usuarios que son miembros de los grupos CityWideOperator y CityWideExecutive.
9. Opcional: Realice uno de los pasos siguiente según sea necesario:
   - En el campo **Se refiere a alertas** , entre una lista de identificadores de sucesos CAP separados por punto y coma a los que hace referencia la nueva alerta.
   - En el campo **Se refiere a KPI** , entre una lista de KPI separados por punto y coma a los que hace referencia la nueva alerta.
10. Pulse **Enviar notificación**.

Conceptos relacionados:

"Notificaciones" en la página 293
Utilice el portlet Notificaciones para ver sus mensajes de alerta y sus detalles.

Script de suceso

Utilice el portlet Script de suceso para escribir un script para crear una lista secuencial de sucesos que se van a publicar a intervalos de tiempo predefinidos.

Para iniciar el portlet Script de suceso, en la interfaz de administración de WebSphere Portal haga clic en **Intelligent Operations** > **Herramientas de demostración** > **Scripts de sucesos**.

En el portlet Script de suceso , puede escribir un script que haga referencia a sucesos que se publicarán por los ID de suceso que se registran en tabla de sucesos de muestra en Base de datos de IBM Intelligent Operations Center. En el script, puede especificar un retraso entre los sucesos que se publiquen. Cuando se ejecuta el script, el sistema publica los sucesos a través del programa de fondo. Sin embargo, el flujo de suceso es el mismo que para los sucesos que entra el sistema desde fuentes externas.

También puede borrar sucesos desde Base de datos de IBM Intelligent Operations Center. Si borra los sucesos desde Base de datos de IBM Intelligent Operations Center, se suprimen todos los sucesos que se visualizan en el portlet Mapa y en el portletDetalles .

Antes de que utilice el portlet Script de suceso , puede ver los sucesos en tabla de sucesos de muestra en Base de datos de IBM Intelligent Operations Center.

En el portlet Script de suceso , siga el ejemplo para crear un script JSON que defina la lista de sucesos secuencial que se va a publicar a intervalos de tiempo predefinidos. Antes de ejecutar el script, debe borrar y validar el script pulsando el botón **Borrar y validar** .

Puede publicar un suceso con un ID particular una sola vez. Debe suprimir todos los sucesos de la Base de datos de IBM Intelligent Operations Center antes de volver publicar un suceso con el mismo ID. Sin embargo, si selecciona la casilla de verificación **Selección aleatoria de ID**, el portlet de script de suceso publica los mismos sucesos otra vez y aplica ID aleatorios a los sucesos.

Visualización de sucesos de muestra y sucesos de KPI en tabla de sucesos de muestra

El portlet Script de suceso publica sucesos de muestra desde el tabla de sucesos de muestra de Base de datos de IBM Intelligent Operations Center. Utilice el siguiente procedimiento para ver los sucesos en tabla de sucesos de muestra.

Procedimiento

1. Utilice un cliente VNC para iniciar sesión en servidor de datos como usuario raíz y, a continuación, abra una ventana de mandatos. En los pasos siguientes, entre mandato en la ventana de mandatos que acaba de abrir en servidor de datos.
2. Para poder abrir DB2 Control Center, debe apagar temporalmente el control de acceso; entre el siguiente mandato: `xhost +`
3. En DB2 Control Center, vea los sucesos de muestra que están en tabla de sucesos de muestra, y obtenga los números ID de suceso de muestra:
   a. Para abrir DB2 Control Center, introduzca los mandatos siguientes:
      ```
      su - db2inst1
      db2cc
      ```
   b. En DB2 Control Center, pulse **Todas las bases de datos** > **IOCDB** > **Tablas** > **REF_SAMPLEEVENTS**.
   c. Pulse con el botón derecho del ratón en la tabla **REF_SAMPLEEVENTS** y, a continuación, pulse **Abrir**. Hay 40 filas en tabla de sucesos de muestra, pero una vez se han publicado los sucesos, solo se muestran los sucesos 1-8 en el portlet Detalles . Los demás sucesos son para probar KPI. Si seleccione la casilla de verificación **Aleatorizar ID** en el portlet Script de suceso , puede publicar los mismos ocho sucesos repetidamente.
   d. Tenga en cuenta **SAMPLEID** para cada suceso de muestra, para hacer referencia al crear scripts de sucesos en el portlet Script de suceso . El valor de **SAMPLEID** corresponde al ID del suceso.
4. Cuando termine de visualizar los sucesos de muestra, cierre DB2 Control Center.
5. Para cambiar de vuelta al usuario raíz, entre el siguiente mandato: `exit`
6. Para activar de nuevo el control de acceso, entre el siguiente mandato: `xhost -`

Conceptos relacionados:

"KPI de muestra" en la página 125
Los KPI de muestra se proporcionan con IBM Intelligent Operations Center. Los KPI de muestra están diseñados para facilitar la implementación de distintos tipos de KPI utilizando IBM WebSphere Business Monitor Development Toolkit. Se proporcionan modelos de supervisión de muestra para agua, transporte y seguridad pública.

Creación de un script de suceso

Cree un script de suceso que publique una secuencia de sucesos a intervalos de tiempo predefinidos.

Antes de empezar

Antes de utilizar el portlet Script de suceso para publicar sucesos, puede ver esos sucesos en tabla de sucesos de muestra en Base de datos de IBM Intelligent Operations Center.

Acerca de esta tarea

Utilice los pasos siguientes para crear un script de suceso en el portlet Script de suceso .

Nota: Puede publicar un suceso con un ID particular una sola vez. Para poder publicar un suceso con el mismo ID de nuevo, pulse **Restablecer base de datos** para suprimir todos los sucesos desde Base de datos de IBM Intelligent Operations Center. Por otra parte, para publicar los mismos sucesos de nuevo con ID aleatorios aplicados, seleccione la casilla de verificación **Aleatorizar ID** .

Procedimiento

1. En la interfaz de administración de WebSphere Portal, pulse **Intelligent Operations** > **Herramientas de demostración** > **Scripts de sucesos**.
2. Utilice el ejemplo datos en el portlet Script de suceso para crear un script JSON que define una lista de sucesos secuencial que se publicará a intervalos de tiempo predefinidos; entre el script en el campo de la parte izquierda del ejemplo. El script JSON de ejemplo mostrado en el portlet Script de suceso también se visualiza en el siguiente código:

```
[
    {
        "id": 2
        //ID of element in Sample Events table
        "delayAfter": 4000
        //Milliseconds to wait after publishing the event with the current ID
    },
    {}, //Empty objects are ignored
    {
        "id": 1
        //If the command specifies only an ID, the next command is processed
        //directly after the previous command
    },
    {
        "delayAfter": 0
        //If the command specifies only a delay, no event is published and the
        //script waits until the next command is due
    }
]
```

3. Opcional: Para publicar los mismos sucesos de nuevo con ID aleatorios aplicados, seleccione la casilla de verificación **Aleatorizar ID** .
4. Necesario: Para limpiar y validar el script antes de ejecutarlo, pulse **Limpiar y validar**. La sintaxis del script se valida y los comentarios se eliminan. Si se detecta un marcado incorrecto en el script que no se puede resolver, se visualiza un mensaje.
5. Para ejecutar el script, pulse **Ejecutar script de suceso**.
6. Para eliminar todos los sucesos de Base de datos de IBM Intelligent Operations Center e impedir que el script publique más sucesos, pulse **Restablecer base de datos**.

Tareas relacionadas:

"Visualización de sucesos de muestra y sucesos de KPI en tabla de sucesos de muestra" en la página 112
El portlet Script de suceso publica sucesos de muestra desde el tabla de sucesos de muestra de Base de datos de IBM Intelligent Operations Center. Utilice el siguiente procedimiento para ver los sucesos en tabla de sucesos de muestra.

Creación e integración de KPI

Los modelos de KPI se pueden crear y modificar utilizando un kit de herramientas de desarrollo de supervisión de negocio y un portlet de gestión de KPI.

El kit de herramientas de desarrollo de IBM WebSphere Business Monitor se puede instalar con Rational Application Developer, ambos se incluyen con IBM Intelligent Operations Center. El kit de herramientas de desarrollo de IBM WebSphere Business Monitor también está instalado con WebSphere Integration Developer.

Antes de definir o modificar un KPI debe entender en que se basará la alerta CAP de Protocolo Común de Alertas (CAP). Por ejemplo, si está definiendo un KPI haciendo un seguimiento del nivel de un origen de agua, necesitará conocer los elementos CAP que contienen los elementos que tiene que rastrear, como el nombre del origen de agua y la profundidad del agua. Cuando se haya añadido o modificado un KPI de este modo, se debe desplegar en el servidor de IBM WebSphere Business Monitor.

Para obtener información adicional sobre cómo utilizar IBM WebSphere Business Monitor y el kit de herramientas de desarrollo de IBM WebSphere Business Monitor, consulte IBM WebSphere Business Monitor Information Center.

Cuando se han establecido modelos y métricas de KPI a través de IBM WebSphere Business Monitor, puede utilizar el portlet de Indicadores clave de rendimiento para desarrollar y modificar los KPI.

Conceptos relacionados:

"KPI de muestra" en la página 125
Los KPI de muestra se proporcionan con IBM Intelligent Operations Center. Los KPI de muestra están diseñados para facilitar la implementación de distintos tipos de KPI utilizando IBM WebSphere Business Monitor Development Toolkit. Se proporcionan modelos de supervisión de muestra para agua, transporte y seguridad pública.

"Sucesos y KPI" en la página 95
sucesos de proceso de IBM Intelligent Operations Center e indicadores de rendimiento clave (KPI) para determinar cómo se muestra la información.

"Personalización de los ICR" en la página 172
En IBM Intelligent Operations Center, puede personalizar los modelos de indicador clave de rendimiento (KPI) para que se adapten a sus procesos empresariales.

Referencia relacionada:

"Instalación de herramientas proporcionadas con la solución" en la página 66
Los kits de herramientas y las herramienta de desarrollo se incluyen con IBM Intelligent Operations Center. Se utilizan al personalizar IBM Intelligent Operations Center.

Información relacionada:

Centro de información de IBM WebSphere Business Process Management Versión 7.0

Modelos de supervisión y KPI

Un modelo de supervisión define métricas e indicadores clave de rendimiento (KPI), sus dependencias en sucesos de entrada, condiciones que requieren acciones empresariales y sucesos de salida que informan de las condiciones que pueden desencadenar acciones empresariales.

Un modelo de supervisión puede contener los siguientes submodelos:

- Modelo de detalles de supervisión
- Modelo de ICR
- Modelo dimensional
- Modelo visual
- Modelo de suceso

El modelo de detalles de supervisión contiene la mayoría de la información del modelo de supervisión.

Los modelos de supervisión de muestra proporcionados por IBM Intelligent Operations Center no utilizan modelos visuales o dimensionales.

El modelo de detalles de supervisión define uno o más contextos de supervisión. Un contexto de supervisión define la información que se va a recopilar y supervisar desde uno o más sucesos de entrada. Las entradas supervisadas de IBM Intelligent Operations Center son alertas CAP. La información recopilada desde estas alertas se utiliza para calcular un KPI.

El modelo de KPI contiene uno o más contextos de KPI. Estos definen los KPI y sus sucesos y desencadenantes asociados. Los contextos de KPI pueden procesar sucesos de entrada, evaluar desencadenantes de tiempo de espera recurrentes y enviar sucesos salientes. Por ejemplo, el contexto puede comprobar si un KPI está fuera del rango definido y envía una notificación.

El modelo de suceso hace referencia a todas las definiciones de entrantes y salientes utilizadas en el modelo de supervisión. Se refiere a esquemas que describen la estructura de partes de sucesos individuales.

Conceptos relacionados:

"KPI de muestra" en la página 125
Los KPI de muestra se proporcionan con IBM Intelligent Operations Center. Los KPI de muestra están diseñados para facilitar la implementación de distintos tipos de KPI utilizando IBM WebSphere Business Monitor Development Toolkit. Se proporcionan modelos de supervisión de muestra para agua, transporte y seguridad pública.

Información relacionada:

Information Center de IBM Business Monitor

Instancias de contexto de supervisión

Una instancia de contexto de supervisión es información recopilada en un punto específico en el tiempo dentro de un contexto de supervisión.

Para IBM Intelligent Operations Center una instancia de contexto de supervisión se corresponde con una alerta CAP. Cuando se recibe una alerta CAP, se crea una instancia de contexto de supervisión o se vuelve a utilizar, y las métricas dentro de esa instancia de contexto se llenan con los valores de alerta CAP basados en el contexto de supervisión.

Se puede definir un contexto de supervisión para crear una instancia nueva para cada una de las alertas CAP o volver a utilizar una instancia existente. Por ejemplo, si quiere que un KPI calcule el nivel de agua de media semanal para un recurso determinado dentro del nivel de agua muestreado diariamente, debe crear una instancia de contexto de supervisión nueva para cada alerta CAP. Cada instancia debe contener el nivel de agua diario y el KPI debe calcular el promedio de las medidas en un periodo de siete días.

Los KPI se calculan utilizando las métricas definidas para un contexto de supervisión. Al definir un KPI de agregación, especifica el contexto de supervisión y la métrica utilizada como entrada para la función de agregación de KPI. Cuando se evalúa el KPI, la función de agregación utiliza los valores de métrica para las instancias de contexto supervisadas para calcular el valor de KPI.

Conceptos relacionados:

"KPI de muestra" en la página 125
Los KPI de muestra se proporcionan con IBM Intelligent Operations Center. Los KPI de muestra están diseñados para facilitar la implementación de distintos tipos de KPI utilizando IBM WebSphere Business Monitor Development Toolkit. Se proporcionan modelos de supervisión de muestra para agua, transporte y seguridad pública.

Información relacionada:

Information Center de IBM Business Monitor

Modelado de ICR

Los KPI de modelo con Rational Application Developer o WebSphere Integration Developer, con el kit de herramientas de desarrollo IBM WebSphere Business Monitor instalado. Rational Application Developer y el kit de herramientas de desarrollo de IBM WebSphere Business Monitor se incluyen como parte de IBM Intelligent Operations Center.

Acerca de esta tarea

Los KPI se modelan utilizando Rational Application Developer o WebSphere Integration Developer, con el kit de herramientas de desarrollo IBM WebSphere Business Monitor. Para obtener más información sobre el uso de estas herramientas, consulte los centros de información de los productos correspondientes.

Los modelos de supervisión se encuentran dentro de los proyectos de supervisión empresarial. Los modelos y proyectos se crean utilizando los asistentes de supervisión empresarial de Rational Application Developer proporcionados con el kit de herramientas de desarrollo de IBM WebSphere Business Monitor.

Para modelar un KPI, haga lo siguiente.

Procedimiento

1. Entienda la alerta CAP que va a recibir IBM Intelligent Operations Center.
2. Entienda el propósito del KPI. ¿Generará el KPI una acción si se alcanza o se supera el límite? ¿Se utilizará el KPI para calcular datos estadísticos o históricos?
3. Determine el nombre para el contexto de supervisión. La convención de denominación de IBM Intelligent Operations Center va a utilizar el tipo de suceso CAP como nombre. Los ejemplos proporcionados por IBM Intelligent Operations Center crean un contexto de supervisión aparte para cada mensaje de alerta CAP enviado a IBM WebSphere Business Monitor.
4. En Rational Application Developer o WebSphere Integration Developer, con Kit de herramientas de desarrollo de IBM WebSphere Business Monitor instalado, defina el suceso entrante, la clave y el conjunto de métricas del contexto del supervisor. El suceso de entrada define el mensaje de alerta CAP supervisado por el contexto, una clave que define exclusivamente la instancia de contexto y las métricas que definen la información extraída del mensaje de alerta CAP.
5. Especifique el esquema CAP para el suceso. El esquema debe existir en el proyecto de supervisión. El IBM Intelligent Operations Center proporciona una copia del esquema CAP v1.2 en el proyecto de modelado `icoc_sample_monitor_models` de ejemplo.
6. Especifique el nombre e ID para cada uno de los sucesos de entrada de supervisión empresarial. Los ID de suceso no pueden contener espacios o caracteres especiales. De forma predeterminada, el ID se crea a partir del nombre con guiones bajos sustituidos por espacios. Todos los ejemplos proporcionados por IBM Intelligent Operations Center utilizan ID de elemento predeterminados.
7. Especifique el esquema. El esquema define la estructura del suceso de entrada para IBM WebSphere Business Monitor.
8. Defina el filtrado deseado de los mensajes CAP. Por ejemplo, limite la supervisión a tipos de suceso específicos o gravedad.
9. Especifique las métricas a extraer desde el mensaje CAP.

10. Defina una clave de contexto para identificar de forma exclusiva la instancia de contexto de supervisión. Los valores clave se especifican por medio del suceso de entrada cuando se crea el contexto de supervisión.
11. Especifique si se deben correlacionar los sucesos de entrada.
12. Especifique el contexto de KPI. Un contexto de KPI es un contenedor para KPI y sus sucesos y desencadenadores asociados. A diferencia de un contexto de supervisión, un contexto de KPI no contiene claves o métricas. Un contexto de KPI debe crearse como contenedor antes de crear ningún KPI.
13. Cree un KPI dentro del contexto de KPI definido previamente.
14. Especifique el tipo de KPI: **Decimal** o **Duración**.
15. Defina los rangos, valores e indicadores de color del KPI. La mayoría de los KPI IBM Intelligent Operations Center de muestra definen tres rangos y colores asociados.

Tabla 34. Definiciones de color y rango de KPI de muestra

Nombre	**Color**	**RGB**
Aceptable	verde	699037
Precaución	amarillo	FDBA1A
Tomar medida	rojo	C32E14

16. Defina cómo se calcula un KPI. Los valores de KPI se determinan de una de estas dos formas. Si el valor proviene de una métrica utilizando una función de agregación, se hará referencia al KPI como KPI agregado. Si el valor se calcula en base a otros KPI o a funciones XPath definidas por el usuario, se hace referencia al KPI como un KPI de expresión.

    En las muestras de IBM Intelligent Operations Center, los KPI de nivel inferior (KPI sin hijos) se definen como KPI agregados. Los KPI de nivel más alto (KPI con hijo) se definen como KPI de expresión.

    Los valores de los KPI agregados se calculan a partir de métricas llenas de datos enviados en mensajes de alerta CAP enviados al servidor IBM WebSphere Business Monitor . Después, se ejecuta una función de agregación en estos datos. Las funciones de agregación incluyen:

    - `promedio`
    - `máximo`
    - `mínimo`
    - `suma`
    - `número de apariciones`
    - `desviación estándar`

    Los valores se expresan como medidas cuantificables. Por ejemplo, el tiempo medio de respuesta de un crimen (5 minutos, 7 segundos) o el nivel medio de agua (100,5).

    Los valores KPI de expresión se calculan a partir de cálculos y rangos. En las muestras deIBM Intelligent Operations Center, los KPI padre tienen cálculos que causan que el KPI evalúe en un valor de 0, 1 o 2 en función de los valores de los KPI hijos. Un valor de 0 se correlaciona con un rango aceptable, 1 con un rango de precaución y 2 con un rango para tomar medidas. Los ejemplos utilizan expresiones de cálculo para establecer el valor de KPI en la urgencia más alta de sus hijos.
17. Opcional: Especifique el filtro de tiempo para un KPI agregado. Los KPI de agregación tienen filtros de tiempo opcionales que limitan el periodo de tiempo sobre cuál es el valor KPI calculado. El periodo de tiempo puede ser un intervalo repetido (por ejemplo, el último periodo actual o completo), un intervalo continuado o un intervalo fijo. Todos los KPI agregados de IBM Intelligent Operations Center de muestra tiene filtros de tiempo definidos.
18. Opcional: Especifique un filtro de datos para el KPI. Por ejemplo, si el tiempo de respuesta medio de un crimen se calcula con Police Precinct One y no con otro precinto, se puede utilizar un filtro de datos para eliminar los demás contextos de supervisión.

19. Defina cómo se actualizan los valores KPI incluyendo desencadenadores, sucesos de entrada al servidor IBM WebSphere Business Monitor y sucesos de salida a IBM Intelligent Operations Center.
20. Pruebe el KPI. El kit de herramientas de desarrollo de IBM WebSphere Business Monitor tiene un entorno de prueba para probar los KPI antes del despliegue. Para conocer más detalles siga el enlace situado al final de este tema.
21. Despliegue la aplicación de modelo de supervisión.

Conceptos relacionados:

"Definición de jerarquías KPI"
Puede definir relaciones padre-hijo entre KPI y diseñar cómo se muestran los KPI en IBM Intelligent Operations Center. Diseñe sus propias jerarquías KPI para que pueda buscar KPI de manera que se adapte a su proceso de negocio.

"KPI de muestra" en la página 125
Los KPI de muestra se proporcionan con IBM Intelligent Operations Center. Los KPI de muestra están diseñados para facilitar la implementación de distintos tipos de KPI utilizando IBM WebSphere Business Monitor Development Toolkit. Se proporcionan modelos de supervisión de muestra para agua, transporte y seguridad pública.

"Comunicación de sucesos de KPI entre IBM WebSphere Business Monitor y IBM Intelligent Operations Center" en la página 120
IBM WebSphere Business Monitor puede enviar sucesos salientes desde un contexto de KPI o de supervisión a IBM Intelligent Operations Center.

Tareas relacionadas:

"Despliegue de modelos de supervisión" en la página 123
Después de definir los indicadores clave de rendimiento (KPI) y sus modelos de supervisión, el supervisor tiene que desplegarse para el IBM WebSphere Business Monitor que se está ejecutando enIBM Intelligent Operations Center servidor de aplicaciones.

Referencia relacionada:

"Instalación de herramientas proporcionadas con la solución" en la página 66
Los kits de herramientas y las herramienta de desarrollo se incluyen con IBM Intelligent Operations Center. Se utilizan al personalizar IBM Intelligent Operations Center.

Información relacionada:

Information Center de Rational Application Developer

Information Center de IBM Business Monitor

XML Path Language (XPath) 2.0 (segunda edición)

Definición de jerarquías KPI

Puede definir relaciones padre-hijo entre KPI y diseñar cómo se muestran los KPI en IBM Intelligent Operations Center. Diseñe sus propias jerarquías KPI para que pueda buscar KPI de manera que se adapte a su proceso de negocio.

Mientras que IBM WebSphere Business Monitor permite un KPI basado en el valor de otro KPI, no permite la definición de una relación padre-hijo entre KPI. Para simplificar esta tarea, IBM Intelligent Operations Center proporciona un portlet de Indicadores clave de rendimiento para el administrador. Para obtener más información acerca de este portlet, consulte el enlace al final de este tema.

Los KPI de muestra IBM Intelligent Operations Center definen una serie de KPI de Police Department con un diseño jerárquico de la siguiente manera:

```
Police Department  ---------------------------- level 1
   Crime Response Time ------------------------- level 2
      Crime Response Time Precinct One ----- level 3
      Crime Response Time Precinct Two ----- level 3
```

En este caso Police Department tiene un hijo: Crime Response Time. Crime Response Time tiene dos hijos: Crime Response Time Precinct One y Crime Response Time Precinct Two.

Los dos KPI de nivel 3 se definen en el modelo de KPI como KPI agregados. Es decir, sus valores se calculan utilizando un valor de métrica y una función de agregación. Todos los demás KPI de este conjunto son KPI de expresión con sus valores calculados desde los valores de otros KPI. Por ejemplo:

- Crime Response Time se basa en los valores de Crime Response Time Precinct One y Crime Response Time Precinct Two.
- Police Department se basa en el valor de Crime Response Time.

IBM Intelligent Operations Center soporta una alternativa al uso del portlet de Indicadores clave de rendimiento para definir relaciones de KPI. El portlet deIndicadores clave de rendimiento es el método predeterminado con el parámetro **UseDBModelReader** establecido en true en tabla de propiedades del sistema. Para obtener información sobre cómo cambiar la configuración en tabla de propiedades del sistema, pulse el enlace al final de este tema. Para obtener información acerca del método alternativo para definir las relaciones de KPI, pulse el enlace al final de este tema.

Conceptos relacionados:

"Indicadores clave de rendimiento" en la página 173
Utilice el portlet Indicadores clave de rendimiento para personalizar los indicadores clave de rendimiento (ICR) y su visualización jerárquica en IBM Intelligent Operations Center.

"Especificación de datos de configuración de todo el sistema" en la página 182
La tabla de propiedades del sistema IBM Intelligent Operations Center almacena datos de configuración IBM Intelligent Operations Center .

"Definición de las jerarquías de KPI con OWL"
IBM Intelligent Operations Center soporta el uso de OWL (Web Ontology Language), como alternativa al uso del portlet de Indicadores clave de rendimiento para definir las relaciones padre-hijo de KPI.

Definición de las jerarquías de KPI con OWL

IBM Intelligent Operations Center soporta el uso de OWL (Web Ontology Language), como alternativa al uso del portlet de Indicadores clave de rendimiento para definir las relaciones padre-hijo de KPI.

Las relaciones padre-hijo de KPI se pueden definir en OWL que IBM Intelligent Operations Center lee y procesa. Las definiciones se almacenan en un archivo RDF (Resource Description Framework).

Puede especificar si el modelo de base de datos KPI debe leerse o no desde un archivo RDF. Para obtener más información sobre cómo cambiar esta propiedad en tabla de propiedades del sistema, consulte el enlace situado al final de este tema.

Un ejemplo de definiciones OWL para el conjunto de KPI de muestra Police Department es como sigue:

```
<icop:KPIDefinition rdf:ID="Police_Department">
<icop:KPIBase.name>Police Department</icop:KPIBase.name>
<icop:KPIBase.id>Police_Department</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_ModelDefinition
      rdf:resource= "#icoc_sample_public_safety_monitor_model"/>
</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time">
<icop:KPIBase.name>Crime Response Time</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Police_Department"/>
</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_One">
<icop:KPIBase.name>Crime Response Time Precinct One</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_One</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >
```

```
<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_Two">
<icop:KPIBase.name>Crime Response Time Precinct Two</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_Two</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >
```

Nota: OWL es un lenguaje compilado en RDF. OWL y RDF son similares, pero OWL es un lenguaje más fuerte. OWL proporciona un vocabulario más amplio, sintaxis más fuerte y una mayor interpretabilidad que RDF.

Conceptos relacionados:

"Definición de jerarquías KPI" en la página 118
Puede definir relaciones padre-hijo entre KPI y diseñar cómo se muestran los KPI en IBM Intelligent Operations Center. Diseñe sus propias jerarquías KPI para que pueda buscar KPI de manera que se adapte a su proceso de negocio.

"Indicadores clave de rendimiento" en la página 173
Utilice el portlet Indicadores clave de rendimiento para personalizar los indicadores clave de rendimiento (ICR) y su visualización jerárquica en IBM Intelligent Operations Center.

"Especificación de datos de configuración de todo el sistema" en la página 182
La tabla de propiedades del sistema IBM Intelligent Operations Center almacena datos de configuración IBM Intelligent Operations Center .

Comunicación de sucesos de KPI entre IBM WebSphere Business Monitor y IBM Intelligent Operations Center

IBM WebSphere Business Monitor puede enviar sucesos salientes desde un contexto de KPI o de supervisión a IBM Intelligent Operations Center.

Los sucesos salientes desde el servidor IBM WebSphere Business Monitor están colocados en una cola de mensajes externa. El IBM Intelligent Operations Center utiliza este mecanismo para recibir de forma asíncrona actualizaciones de KPI.

Nota: Puede especificar si la conexión a IBM WebSphere Business Monitor es para utilizar SSL para una conexión segura. Para obtener más información sobre cómo cambiar esta propiedad en la tabla de propiedades del sistema, consulte el enlace al final del tema.

Conceptos relacionados:

"Especificación de datos de configuración de todo el sistema" en la página 182
La tabla de propiedades del sistema IBM Intelligent Operations Center almacena datos de configuración IBM Intelligent Operations Center .

"Uso de la cola de sucesos de entrada definida por IBM Intelligent Operations Center" en la página 104
Se pueden publicar sucesos CAP en IBM Intelligent Operations Center dirigiéndolos a la instancia de WebSphere Message Broker incluida.

Desencadenantes

Un desencadenador es un mecanismo que detecta una indicencia y puede provocar un procesamiento adicional en respuesta a esa incidencia.

Las muestras de KPI proporcionadas con IBM Intelligent Operations Center definen dos tipos de desencadenadores. El primer desencadenador se dispara cuando el servidor IBM WebSphere Business Monitor recibe un mensaje de alerta CAP, también conocido como suceso de entrada para un conjunto de KPI definido. El mensaje de alerta de la PAC podría, o no, cambiar el KPI. El IBM Intelligent Operations Center determina si se cambia el KPI cuando se recibe la notificación de sucesos desde el servidor IBM WebSphere Business Monitor .

Para sucesos salientes, un desencadenador determina cuándo se enviará el suceso.

Se pueden utilizar sucesos basados en desencadenadores para enviar notificaciones aIBM Intelligent Operations Center cuando cambia la entrada para un cálculo de KPI. Sin embargo, los desencadenadores de sucesos no se pueden utilizar para dirigir la situación cuando cambia un valor de KPI después de que caduca un periodo de tiempo definido. En los ejemplos de IBM Intelligent Operations Center , se utilizan desencadenadores basados en tiempo para enviar notificaciones a IBM Intelligent Operations Center para aquellos KPI con definiciones de periodo de tiempo cortos.

Por ejemplo, el `Severe Traffic Accidents KPI` se define para que caduque cada hora. Si el KPI tiene un valor de 3 a las 10:00 y no se han recibido mensajes de alerta CAP para ese KPI durante la siguiente hora, el periodo de tiempo caduca y el valor de KPI se restablece a 0.

Definición de los sucesos de entrada para IBM WebSphere Business Monitor

En las muestras de IBM Intelligent Operations Center , se utilizan los sucesos de entrada para determinar cuando se inicia un desencadenador. Los sucesos de entrada para un contexto KPI se definen de forma similar a aquellos supervisados por un contexto de supervisión.

Acerca de esta tarea

Los sucesos entrantes se definen utilizando Rational Application Developer or WebSphere Integration Developer con Kit de herramientas de desarrollo de IBM WebSphere Business Monitor. Para obtener más información sobre cómo utilizar estas herramientas, consulte los Information Center de estos productos.

Para definir un suceso de entrada, haga lo siguiente.

Procedimiento

1. Seleccione el contexto KPI para el suceso de entrada.
2. Cree un suceso de entrada y especifique el nombre e ID del suceso.
3. Especifique el esquema CAP.
4. Especifique la condición de filtro.
5. Seleccione el contexto KPI y cree un suceso de entrada nuevo.
6. Cree un desencadenador nuevo para el suceso de entrada.
7. Asegúrese de que el desencadenador se puede repetir para que el desencadenador se inicie cada vez que se actualice el origen desencadenante y se cumpla la condición del desencadenador.
8. Seleccione el origen del desencadenador.
9. Defina la condición de desencadenante. Cuando se cumple la condición de desencadenantes, se inicia el desencadenador.

Ejemplo

Los modelos de supervisión de IBM Intelligent Operations Center de muestra se definen para que el desencadenador se inicie cada vez que se recibe un mensaje de alerta CAP a través de servidor de IBM WebSphere Business Monitor .

Tareas relacionadas:

"Modelado de ICR" en la página 116
Los KPI de modelo con Rational Application Developer o WebSphere Integration Developer, con el kit de herramientas de desarrollo IBM WebSphere Business Monitor instalado. Rational Application Developer y el kit de herramientas de desarrollo de IBM WebSphere Business Monitor se incluyen como parte de IBM Intelligent Operations Center.

Información relacionada:

Information Center de IBM Business Monitor

Information Center de Rational Application Developer

Definición de sucesos salientes a IBM Intelligent Operations Center

Los sucesos salientes definen la información enviada desde IBM WebSphere Business Monitor a IBM Intelligent Operations Center cuando se activa un desencadenador.

Acerca de esta tarea

El IBM Intelligent Operations Center utiliza notificaciones salientes enviadas desde el servidor IBM WebSphere Business Monitor para determinar si el KPI ha cambiado. Si el KPI ha cambiado, el IBM Intelligent Operations Center obtiene los datos KPI desde el servidor IBM WebSphere Business Monitor , actualiza la información de caché del KPI y actualiza los datos de IBM Intelligent Operations Center .

Los sucesos salientes se definen utilizando Rational Application Developer o WebSphere Integration Developer con Kit de herramientas de desarrollo de IBM WebSphere Business Monitor. Para obtener más información sobre cómo utilizar estas herramientas, consulte los Information Center de estos productos.

Para definir un suceso saliente, realice los pasos siguientes.

Procedimiento

1. Seleccione el contexto de KPI para el suceso saliente.
2. Cree un suceso saliente y especifique el ID y nombre de suceso.
3. Especifique el esquema de notificación. El esquema se ubica en el archivo `ioc-notification-v1.0.xsd` . El esquema está ubicado en el proyecto `icoc_sample_monitor-models` .
4. Defina el contenido del suceso saliente. El contenido se basa en el esquema de notificación.
5. En **notificación**, para el valor de **sentfrom** entre `Supervisar`.
6. Añada los elementos de parámetro al contenido de suceso, como se define en los siguientes subpasos:
   a. Para el primer parámetro, especifique `modelID` para **parameterName** y el ID del modelo de supervisión para **parameterValue**. Por ejemplo, `icoc_sample_public_safety_monitor_model`.
   b. Para cada KPI del conjunto de KPI, añada parámetros para especificar el ID de KPI y el valor de KPI. El ID de KPI se especifica utilizando el elemento **parameterName** y el valor KPI se especifica utilizando el elemento `parameterValue` . El ID de KPI debe estar asociado con un KPI en el conjunto de KPI. Utilice la función `xs:string()` para especificar el valor KPI como una cadena. Por ejemplo, **parameterName** puede ser `Police_Department` y **parameterValue** puede ser `xs:string(Police_Department)`.

Ejemplo

A continuación, se muestra un ejemplo de notificación que se va a enviar a IBM Intelligent Operations Center:

```
<ns1:notification>
  <ns1:notificationType> Alert</ns1:notificationType>
  <ns1:sentFrom> Monitor</ns1:sentFrom>
  <ns1:headline> Police Department KPI Changed</ns1:headline>
```

```
  <ns1:description> Police Department KPI Changed</ns1:description>
  <ns1:kpiLink> Police Department</ns1:kpiLink>
  <ns1:category> Safety</ns1:category>
  <ns1:parameter>
    <ns1:parameterName> modelId</ns1:parameterName>
  <ns1:parameterValue>
     icoc_sample_public_safety_monitor_model</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Police_Department</ns1:parameterName>
    <ns1:parameterValue> 0</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time</ns1:parameterName>
    <ns1:parameterValue> 0</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time_Precinct_One</ns1:parameterName>
    <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time_Precinct_Two</ns1:parameterName>
    <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
  </ns1:parameter>
</ns1:notification>
```

Tareas relacionadas:

"Modelado de ICR" en la página 116
Los KPI de modelo con Rational Application Developer o WebSphere Integration Developer, con el kit de herramientas de desarrollo IBM WebSphere Business Monitor instalado. Rational Application Developer y el kit de herramientas de desarrollo de IBM WebSphere Business Monitor se incluyen como parte de IBM Intelligent Operations Center.

Información relacionada:

Information Center de IBM Business Monitor

Information Center de Rational Application Developer

Despliegue de modelos de supervisión

Después de definir los indicadores clave de rendimiento (KPI) y sus modelos de supervisión, el supervisor tiene que desplegarse para el IBM WebSphere Business Monitor que se está ejecutando enIBM Intelligent Operations Center servidor de aplicaciones.

Acerca de esta tarea

Para desplegar un modelo de supervisión que utilizará IBM WebSphere Business Monitor, los proyectos Java Enterprise Edition (JEE) deben generarse a partir de los modelos definidos. Una vez se han generado los proyectos JEE, se puede exportar la aplicación del modelo como archivo EAR. El archivo EAR se puede desplegar en el IBM WebSphere Business Monitor que se está ejecutando enIBM Intelligent Operations Center servidor de aplicaciones.

Procedimiento

1. En Rational Application Developer o WebSphere Integration Developer con Kit de herramientas de desarrollo de IBM WebSphere Business Monitor instalado, pulse con el botón derecho del ratón el modelo de supervisión que necesita una generación de proyectos en la pestaña **Explorador empresarial**. Por ejemplo, `icoc_sample_public_safety_monitor_model`.
2. Pulse **Generar proyectos JEE de supervisión**. Se crearán los siguientes proyectos: `modelApplication`, `modelLogic` y `modelModerator`.

3. Exporte la aplicación del modelo de supervisión pulsando con el botón derecho del ratón sobre el proyecto `modelApplication` y pulsando**Exportar** > **EAR**.
4. Pruebe los KPI antes de desplegar el archivo EAR en IBM WebSphere Business Monitor.
5. Despliegue el archivo EAR en el servidor IBM WebSphere Business Monitor utilizando las instrucciones en el Information Center de IBM WebSphere Business Monitor .

Información relacionada:

Information Center de IBM Business Monitor

Information Center de Rational Application Developer

Valores de visualización de KPI

Se pueden utilizar los paquetes de recursos de IBM Intelligent Operations Center para proporcionar valores de visualización alternativos desde los valores proporcionados por los modelos de IBM WebSphere Business Monitor .

Los nombres de rango y los nombres de visualización de KPI se definen en los modelos deIBM WebSphere Business Monitor de muestra proporcionados con IBM Intelligent Operations Center. Ejemplo de los nombres de visualización de KPI son:

- Agua
- Calidad del agua

Ejemplos de los nombres de rango son:

- valor de estado aceptable
- valor de estado precaución
- valor de estado tomar medidas

Cada artefacto, por ejemplo KPI y rango, definido en IBM WebSphere Business Monitor tiene un ID asociado con el nombre de visualización. Los ID no pueden contener espacios mientras que los valores de visualización sí pueden. Los ID se utilizan como claves para buscar valores en un paquete de recursos. El IBM Intelligent Operations Center utiliza estos ID para seleccionar los valores de visualización de KPI. Si no se especifican valores en el paquete de recursos para el ID, se utiliza el valor especificado en la definición deIBM WebSphere Business Monitor .

Los valores de visualización de KPI están ubicados por IBM WebSphere Business Monitor utilizando el lenguaje ISO y los códigos del país del servidor IBM WebSphere Business Monitor . Por ejemplo, un valor de porcentaje KPI se muestra en formato 12,61% cuando el entorno local es `es_ES` y 12,61% cuando es `fr_FR` . Las definiciones del paquete de recursos no se utilizan para estos valores.

El paquete de recursos de las propiedades IBM Intelligent Operations Center predeterminadas `escom.ibm.iss.icoc.rest.monitor.resources.Messages.properties`. Este paquete se puede encontrar en `icoc_rest_monitor_resources_utils`.

Este es un paquete de recursos de ejemplo:

```
kpi.NO.VALUE=No data to determine the KPI value
kpi.RANGE.UNDETERMINED=undetermined
Flood_Control=Flood Control
Water_Levels=Water Levels
Flow_Discharge_City_River=Flow Discharge City River
Water_Level_City_Lake=Water Level City Lake
```

En este ejemplo, los valores de `kpi.NO.VALUE` y `kpi.RANGE.UNDETERMINED` los utilizaIBM Intelligent Operations Center cuando los KPI de IBM WebSphere Business Monitor devuelven un valor nulo. Por ejemplo, el KPI del nivel del agua del lago de la ciudad se define con una repetición del periodo de

tiempo diario basado en el último periodo completo. Si no se reciben CAP para este KPI en domingo, y el KPI se solicita el lunes, se devuelve nulo ya que no hay datos disponibles para el día anterior. El valor de visualización se establece en "No hay datos para determinar el valor de KPI" y el nombre de visualización del rango se establece en "indeterminado".

Las demás entradas, `Flood_Control`, `Water_Levels`, `Flow_Discharge_City_River` y `Water_Level_City_Lake`, definen los valores de visualización para los ID de KPI definidos en el modelo de supervisión de muestra`icoc sample water monitor model` proporcionado por IBM Intelligent Operations Center. Estas entradas pueden especificar texto alternativo desde los valores especificados en el supervisor de IBM WebSphere Business Monitor . Por ejemplo, se puede utilizar el paquete de recursos para proporcionar valores traducidos en lugar de cambiar el modelo mismo.

Conceptos relacionados:

"KPI de muestra"
Los KPI de muestra se proporcionan con IBM Intelligent Operations Center. Los KPI de muestra están diseñados para facilitar la implementación de distintos tipos de KPI utilizando IBM WebSphere Business Monitor Development Toolkit. Se proporcionan modelos de supervisión de muestra para agua, transporte y seguridad pública.

Almacenamiento en antememoria de los KPI

Los valores de configuración de IBM Intelligent Operations Center afectan a cuándo se recuperan los valores de KPI de IBM WebSphere Business Monitor.

El IBM Intelligent Operations Center mantiene los valores de KPI en una memoria caché. De forma predeterminada, los KPI se cargan desde IBM WebSphere Business Monitor a la memoria caché y la memoria caché se renueva de acuerdo al intervalo de tiempo especificado por la propiedad **`KpiCacheRefreshInterval`** de la tabla de propiedades del sistema. Este tiempo de renovación se puede alterar dependiendo de los requisitos para entregar KPI actualizados a IBM Intelligent Operations Center. Para obtener más información sobre cómo cambiar esta configuración en tabla de propiedades del sistema, consulte el enlace al final de este tema.

Tenga en cuenta que cuando se crea un KPI en el portlet de Indicadores clave de rendimiento, las actualizaciones del KPI dependen únicamente de la actualización de la memoria caché. Cuando se define un KPI en IBM WebSphere Business Monitor, se puede definir un mecanismo desencadenante para implementar el proceso adicional en respuesta a los cambios en ese KPI.

Conceptos relacionados:

"Especificación de datos de configuración de todo el sistema" en la página 182
La tabla de propiedades del sistema IBM Intelligent Operations Center almacena datos de configuración IBM Intelligent Operations Center .

KPI de muestra

Los KPI de muestra se proporcionan con IBM Intelligent Operations Center. Los KPI de muestra están diseñados para facilitar la implementación de distintos tipos de KPI utilizando IBM WebSphere Business Monitor Development Toolkit. Se proporcionan modelos de supervisión de muestra para agua, transporte y seguridad pública.

Los KPI de nivel inferior se definen como KPI agregados. Los KPI agregados se calculan desde valores que contienen mensajes de alerta CAP entrantes y una función de agregación como promedio, máximo, mínimo, suma, número de aparaiciones o desviación del estándar. Estos valores se expresan en medidas cuantificables. Los valores KPI de nivel inferior se ubican en el formato adecuado basado en el entorno local del servidor IBM WebSphere Business Monitor . Los KPI de nivel superior se correlacionan con valores basándose en la correlación definida al crear el KPI de muestra.

El valor del KPI de muestra de nivel superior es un número con el mismo color y nivel que la respuesta recomendada. Un valor de 0 es aceptable, un valor de 1 implica precaución y un valor de 2 implica que hay que tomar medidas. El valor de KPI de nivel inferior es una duración, un decimal, un porcentaje o una moneda dependiendo del KPI que represente. Por ejemplo:

- 15% es el valor real de un KPI que representa el porcentaje de vuelos retrasados en un aeropuerto concreto durante un periodo de tiempo.
- 5 minutos, 7 segundos es el valor real de un KPI que representa el tiempo de respuesta medio de un crimen para una ubicación determinada durante un periodo de tiempo.

Los archivos de origen para los modelos de supervisión de IBM Intelligent Operations Center de muestra se proporcionan en un archivo de archivado que se puede importar a Rational Application Developer o WebSphere Integration Developer con el kit de herramientas de IBM WebSphere Business Monitor instalado. El archivo de archivado se puede modificar para cambiar, añadir o suprimir definiciones de KPI. Las definiciones se pueden volver a generar y desplegar paraIBM Intelligent Operations Center.

Los modelos de muestra que vienen con IBM Intelligent Operations Center son:

- `icoc_sample_public_safety_monitor_model`
- `icoc_sample_transportation_monitor_model`
- `icoc_sample_water_monitor_model`

Estos modelos contienen las siguientes muestras de KPI:

- Agua
  - Control de Inundaciones
    - Niveles de agua
      - Flujo de descarga del río de la ciudad
      - Nivel de Agua del lago de la ciudad
  - Gestión del agua
    - Planificación estratégica
      - Fugas de agua
      - Suministro de agua versus demanda
  - Calidad del agua
    - Indicadores físicos
      - Turbiedad
      - pH
- Transporte
  - Aeropuertos
    - Vuelos retrasados
      - Vuelos retrasados del aeropuerto uno
      - Vuelos retrasados del aeropuerto dos
  - Carreteras y tráfico
    - Sucesos en carretera
      - Accidentes de tráfico graves
  - Gestión de transportes
    - Ingresos
      - Puentes y Peajes del túnel
      - Ingresos de las instalaciones de aparcamiento
- Seguridad pública
  - Cuerpo de bomberos

- Lesiones de los bomberos
  - Lesiones de bomberos estación de bomberos uno
  - Lesiones de bomberos estación de bomberos dos

– Departamento de Policía
  - Tiempo de respuesta del crimen
    - Tiempo de respuesta del crimen distrito uno
    - Tiempo de respuesta del crimen distrito dos

– Gestión de la seguridad pública
  - Presupuesto de seguridad pública
    - Presupuesto del departamento de EMS
    - Presupuesto del departamento contra incendios
    - Presupuesto del departamento de policía

Conceptos relacionados:

"Estado" en la página 297
Utilice el portlet Estado para ver el estado de los indicadores clave de rendimiento (ICR) para una única organización o en varias organizaciones.

"Obtención de detalles de indicador clave de rendimiento" en la página 281
Utilice el portlet Obtención de detalles de indicador clave de rendimiento para ver información adicional acerca de una categoría de ICR, el estado de sus ICR subyacentes.

"Creación e integración de KPI" en la página 113
Los modelos de KPI se pueden crear y modificar utilizando un kit de herramientas de desarrollo de supervisión de negocio y un portlet de gestión de KPI.

"Personalización de los ICR" en la página 172
En IBM Intelligent Operations Center, puede personalizar los modelos de indicador clave de rendimiento (KPI) para que se adapten a sus procesos empresariales.

Tareas relacionadas:

"Despliegue de modelos de supervisión" en la página 123
Después de definir los indicadores clave de rendimiento (KPI) y sus modelos de supervisión, el supervisor tiene que desplegarse para el IBM WebSphere Business Monitor que se está ejecutando enIBM Intelligent Operations Center servidor de aplicaciones.

"Visualización de sucesos de muestra y sucesos de KPI en tabla de sucesos de muestra" en la página 112
El portlet Script de suceso publica sucesos de muestra desde el tabla de sucesos de muestra de Base de datos de IBM Intelligent Operations Center. Utilice el siguiente procedimiento para ver los sucesos en tabla de sucesos de muestra.

Configuración de Tivoli Service Request Manager

En la interfaz de usuario de Tivoli Service Request Manager , puede gestionar procedimientos de operación estándar, flujos de trabajo y recursos.

Si añade un prefijo común a los nombres de procedimientos de operación estándar, flujos de trabajo y los recursos, será más fácil filtrar los datos de la búsqueda. Por ejemplo, para los proyectos de cliente, utilice el prefijo común `CX`.

Puede especificar si la conexión a Tivoli Service Request Manager utiliza SSL configurando la propiedad**`TSRMServerSecurityEnabled`** . Para obtener más información acerca de esta propiedad y otras propiedades deTivoli Service Request Manager , vaya al enlace al final del tema.

Conceptos relacionados:

"Servidor de sucesos" en la página 212

"Especificación de datos de configuración de todo el sistema" en la página 182
La tabla de propiedades del sistema IBM Intelligent Operations Center almacena datos de configuración IBM Intelligent Operations Center .

Uso de la interfaz de usuario de Tivoli Service Request Manager

Aprenda a acceder a la interfaz de usuario de Tivoli Service Request Manager . Haga que sea más fácil y rápido usar Tivoli Service Request Manager Start Center personalizándolo con enlaces para las características que más utiliza.

Apertura de aplicaciones Tivoli Service Request Manager

Puede abrir aplicaciones Tivoli Service Request Manager a través de la interfaz de administración de WebSphere Portal , bien a través de las Herramientas de administración de solución o a través del portlet Procedimientos operativos estándar . También puede ver un recurso en Tivoli Service Request Manager a través de la interfaz de IBM Intelligent Operations Center.

Antes de empezar

Para poder ver un recurso en Tivoli Service Request Manager a través de la interfaz IBM Intelligent Operations Center, se debe configurar el inicio de sesión único.

Procedimiento

- Para abrir Tivoli Service Request Manager Start Center a través de la interfaz de administración de WebSphere Portal , utilice los subpasos siguientes:
  1. Pulse **Intelligent Operations** > **Herramientas de administración** > **Consolas de administración**.
  2. Pulse **Administración del procedimiento operativo estándar**.
  3. Inicie la sesión en Tivoli Service Request Manager Start Center como administrador.
- Para abrir las aplicaciones Tivoli Service Request Manager relacionadas con procedimientos de operación estándar, utilice el portlet Procedimientos operativos estándar :
  1. Para abrir el portlet Procedimientos operativos estándar, en la interfaz de administración de WebSphere Portal, pulse **Intelligent Operations** > **Herramientas de personalización** > **Procedimientos operativos estándar**.
  2. Elija una de las opciones siguientes:
     - Para abrir la aplicación Procedimiento operativo estándar, pulse **Procedimientos operativos estándar**.
     - Para abrir la aplicación Matriz de selección de procedimiento operativo estándar, pulse **Matriz de selección de procedimiento operativo estándar**.
     - Para abrir la aplicación de diseñador del flujo de trabajo , pulse **Diseñador de flujo de trabajo**.
- Para ver un recurso en la interfaz de usuario Tivoli Service Request Manager a través de la interfaz IBM Intelligent Operations Center , siga los siguientes pasos:
  1. En el portlet Detalles , de la pestaña **Sucesos e incidencias** , haga doble clic en la fila de la lista de sucesos.
  2. Para ver una lista de los recursos en las proximidades del suceso, pulse **Ver recursos de la zona** y seleccione el radio del área en el que desea centrarse. Se muestra una lista de recursos en la pestaña **Recursos**.
  3. En la pestaña **Recursos** , pulse con el botón derecho del ratón sobre una fila de la lista de recursos y, después, pulse**Propiedades**. El recurso se muestran en Tivoli Service Request Manager, en la pestaña **Recursos** .

  Nota: Para salir completamente de la sesión de Tivoli Service Request Manager, debe cerrar la ventana de navegador web de la interfaz de usuario Tivoli Service Request Manager .

Tareas relacionadas:

"Configuración del inicio de sesión único para servicios de colaboración" en la página 54
Importe la señal de LTPA de SSO WebSphere Portal a servidor de sucesos para permitir que los usuarios acceder a servicios de colaboración sin tener que volver a entrar las credenciales.

Configuración de aplicaciones favoritas en Tivoli Service Request Manager Start Center

Actualice las aplicaciones favoritas en Tivoli Service Request Manager Start Center para que pueda acceder a ellas más fácilmente.

Acerca de esta tarea

Cada usuario de Tivoli Service Request Manager tiene su propioTivoli Service Request Manager Start Center con la propia lista personalizada del usuario en Aplicaciones favoritas.

Procedimiento

1. Para ver Tivoli Service Request Manager Start Center, en la parte superior de la interfaz de usuario de Tivoli Service Request Manager , pulse **Iniciar centro**.
2. En Tivoli Service Request Manager Start Center, pulse el icono **Editar portlet** situado al lado de Aplicaciones preferidas.
3. En la ventana Configuración de aplicaciones favoritas , pulse **Seleccionar aplicaciones**.
4. En la ventana Seleccionar aplicaciones , seleccione las aplicaciones que desea visualizar en Aplicaciones favoritas. La siguiente lista muestra aplicaciones que son útiles para los usuarios de IBM Intelligent Operations Center :

   CRONTASK
   Configuración de tarea cron

   DOMAINADM
   Dominios

   PERSONA
   Personas

   PERSONGR
   Grupos de personas

   PLUSIMTRIX
   Matriz de selección SOP

   PLUSIRES
   Recursos

   PLUSIWO
   Actividades SOP

   USUARIO
   Usuarios

   WFDESIGN
   Workflow Designer
5. Para definir la posición en la que se listan las aplicaciones en Aplicaciones favoritas, realice los pasos siguientes:
   a. En la ventana Configuración de aplicaciones favoritas , seleccione una aplicación.
   b. En el campo **Orden** , entre un número.
6. Para guardar las actualizaciones, pulse **Finalizado**.

Configuración de nuevos usuarios en Tivoli Service Request Manager

Cuando añade un usuario a IBM Intelligent Operations Center, asigna permisos y grupos de personas para el usuario en Tivoli Service Request Manager.

Configuración de Planta de inserción predeterminada

Para que un usuario nuevo puede añadir nuevos recursos y aplicarprocedimientos de operación estándar, debe establecer el Planta de inserción predeterminada para el usuario.

Procedimiento

1. Inicie la sesión en Tivoli Service Request Manager Start Center como administrador.
2. Pulse **Ir a** > **Seguridad** > **Usuarios** .
3. Para buscar por el usuario, en la pestaña **Lista** , del campo **Usuario** , entre algunas o todas las letras del nombre del usuario.
4. En la lista, haga clic en el nombre del usuario y, a continuación, haga clic en la pestaña **Usuario** .
5. En Configuración de usuario, al lado del campo **Sitio de inserción predeterminado** , pulse el icono **Seleccionar valor** .
6. En la ventana Seleccionar valor , busque y pulse el nombre de Planta de inserción predeterminada; por ejemplo, **PMSCRTP**. PMSCRTP es un sitio de muestra instalado con IBM Intelligent Operations Center.
7. Pulse el icono **Guardar usuario**.

Asignación de un usuario a un grupo de seguridad

Añada usuarios a los grupos de seguridad adecuados, para que tengan acceso a las aplicaciones apropiadas en Tivoli Service Request Manager.

Acerca de esta tarea

Para añadir un usuario a un grupo, utilice el siguiente procedimiento.

Procedimiento

1. Inicie la sesión en Tivoli Service Request Manager Start Center como administrador.
2. Pulse **Ir a** > **Seguridad** > **Usuarios** .
3. Para buscar por el usuario, en la pestaña **Lista** , del campo **Usuario** , entre algunas o todas las letras del nombre del usuario.
4. En la lista, haga clic en el nombre del usuario y, a continuación, haga clic en la pestaña **Grupos** .
5. Para buscar el grupo al que desea añadir al usuario, en el campo **Grupo** , entre algunas o todas las letras del nombre del usuario.
6. Si el nombre del grupo necesario no está listado, pulse **Nueva fila**.
7. En Detalle, al lado del campo **Grupo** , pulse el icono **Menú de detalles** y, a continuación, pulse **Seleccionar valor**.
8. En la ventana Seleccionar valor , busque y pulse el nombre del grupo requerido.
9. Pulse el icono **Guardar usuario**.

Asignación de un usuario a grupo de personas

En un procedimiento operativo estándar, se pueden asignar tareas a grupos de personas predefinidos. Un usuario debe ser miembro de un grupo de personas particular para ver las tareas asignadas a grupo de personas.

Antes de empezar

Puede utilizar el grupos de personas de muestra proporcionado durante la instalación de IBM Intelligent Operations Center, o puede crear su propio grupos de personas. Para obtener información sobre cómo crear un grupo de personas en Tivoli Service Request Manager, consulte el Information Center deMaximo Asset Management .

Nota: Asegúrese de que los nombres de todos los grupos de personas tienen la misma longitud. Esto garantiza que los usuarios se asignan únicamente a tareas que están asignadas a los grupos de personas de los que son miembro.

Acerca de esta tarea

Para asignar un usuario a un grupo de personas, utilice el siguiente procedimiento.

Procedimiento

1. Inicie la sesión en Tivoli Service Request Manager Start Center como administrador.
2. Pulse **Ir a** > **Administración** > **Recursos** > **Grupos de personas**.
3. Para buscar por el grupo de personas requerido, en la pestaña **Lista** , del campo **Grupos de personas** , entre algunas o todas las letras del nombre de grupo de personas.
4. En la lista, pulse el nombre del grupo de personas.
5. En la pestaña **Grupo de personas** , en Personas, pulse **Nueva fila**.
6. En detalles, al lado del campo **Persona** , pulse el icono **Menú de detalles** y, a continuación, pulse **Seleccionar valor**.
7. En la ventana Seleccionar valor , busque y pulse el nombre del usuario que desea añadir a grupo de personas.
8. En el campo **Secuencia** , entre el siguiente número incremental disponible.
9. Pulse el icono **Guardar grupo de personas** .

Información relacionada:

Information Center de gestión de activos Maximo

Procedimientos operativos estándar

Puede definir procedimientos de operación estándar y actividades para gestionar sucesos que vienen con IBM Intelligent Operations Center. Utilice el portlet Procedimientos operativos estándar para acceder a las aplicaciones procedimiento operativo estándar, matriz de selección del procedimiento de operación estándar y diseñador del flujo de trabajo en Tivoli Service Request Manager.

Para iniciar el portlet Procedimientos operativos estándar, en la interfaz de administración de WebSphere Portal haga clic en **Intelligent Operations** > **Herramientas de personalización** > **Procedimientos operativos estándar**.

Un procedimiento operativo estándar define una secuencia de actividades que se desencadenan en respuesta a un suceso cuyos parámetros cumple con ciertas condiciones predefinidas, donde cada actividad corresponde a un manual o una tarea automatizada. Puede asignar un flujo de trabajo a una tarea automatizada. Cada actividad se asigna a un grupo propietario, y los usuarios se asignan a un grupo propietario a través de su pertenencia a un grupo de personas. Todos los usuarios asignados al grupo propietario pueden gestionar las actividades a través del portlet Mis actividades .

Puede especificar el orden en el que se ejecutan algunas o todas las actividades de procedimiento operativo estándar . Por ejemplo, puede especificar que no se inicie una actividad particular hasta que se haya completado la actividad anterior o se salte.

Para abrir la aplicación procedimiento operativo estándar, en el portlet Procedimientos operativos estándar haga clic en **Procedimientos operativos estándar**.

Matriz de selección del procedimiento de operación estándar

En matriz de selección del procedimiento de operación estándar, defina los parámetros de sucesos que determinan si procedimiento operativo estándar se ha iniciado para un suceso determinado. Cada procedimiento operativo estándar puede tener uno o más conjuntos de criterios de selección. Sin embargo, cada conjunto de criterios de selección debe ser único.

Para abrir la aplicación matriz de selección del procedimiento de operación estándar, en el portlet Procedimientos operativos estándar haga clic en **Matriz de selección de procedimientos operativos estándar**.

Diseñador del flujo de trabajo

Utilice el diseñador del flujo de trabajo paradiseñar elflujos de trabajo que puede asignarse a las tareas de procedimiento operativo estándar como tareas automatizadas.

Para abrir la aplicación diseñador del flujo de trabajo , en el portlet Procedimientos operativos estándar , pulse **Diseñador de flujo de trabajo**.

Personalización del portlet Procedimientos operativos estándar

Puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Conceptos relacionados:

"Mis actividades" en la página 290
El portlet Mis actividades muestra una lista dinámica de actividades que son propiedad del grupo del que es miembro el usuario que tiene sesión iniciada en la interfaz.

Referencia relacionada:

"Valores del portlet Procedimientos operativos estándar" en la página 168
Personalice el portlet Procedimientos operativos estándar cambiando los valores en los campos de la ventana **Valores compartidos** .

Creación de flujos de trabajo

En Tivoli Service Request Manager, puede crear flujos de trabajo que puede incluir como tareas automáticas en las actividades de procedimiento operativo estándar .

Acerca de esta tarea

Para obtener información detallada sobre cómo crear flujos de trabajo, consulte el enlace al Information Center de Maximo Asset Management al final del tema.

Procedimiento

1. Para abrir el portlet Procedimientos operativos estándar, en la interfaz de administración de WebSphere Portal, pulse **Intelligent Operations** > **Herramientas de personalización** > **Procedimientos operativos estándar**.
2. Para abrir la aplicación de diseñador del flujo de trabajo , pulse **Diseñador de flujo de trabajo**.
3. En la ventana Diseñador de flujo de trabajo , pulse la pestaña **Lienzo** .
4. En la pestaña **Lienzo** , pulse los iconos adecuados para insertar los nodos y flechas necesarios para flujo de trabajo.

Información relacionada:

Information Center de gestión de activos Maximo

Creación de procedimientos de operación estándar

Cree un procedimiento operativo estándar, y asígnelo a un grupo propietario. Los usuarios se asignan a un grupo propietario a través de su pertenencia a un grupo de personas.

Procedimiento

1. Para abrir el portlet Procedimientos operativos estándar, en la interfaz de administración de WebSphere Portal, pulse **Intelligent Operations** > **Herramientas de personalización** > **Procedimientos operativos estándar**.
2. Para abrir la aplicación procedimiento operativo estándar, haga clic en **Procedimientos Operativos Estándar**.
3. En la ventana Procedimiento operativo estándar, en la pestaña **Lista**, pulse el icono **Nuevo SOP**. Se visualizará un procedimiento operativo estándar en blanco en la pestaña **Procedimiento operativo estándar**.
4. Para **Nombre de SOP**, especifique un nombre, y en el campo junto a **Nombre de SOP**, especifique una descripción. Para los nombres de procedimientos de operación estándar, utilice un formato coherente que sea parecido a los nombres del procedimientos de operación estándar de muestra; por ejemplo, `Preparar para evacuación debida a condiciones meteorológicas extremas (Preparar)`. Así mismo, si el último carácter del nombre es un paréntesis, añada la marca de izquierda a derecha (LRM) para evitar problemas potenciales relacionados con la representación de texto bidireccional. Por ejemplo, escriba el nombre utilizado en el ejemplo anterior como `Preparar evacuación en caso de condiciones meteorológicas severas (Preparar)&#x200E;`. El carácter LRM no se visualiza en la interfaz de usuario después de guardar el procedimiento operativo estándar.Además, si añade un prefijo común a los nombres de todos los procedimientos de operación estándar, es más fácil filtrar los procedimientos de operación estándar en una búsqueda. Por ejemplo, para los proyectos de cliente, utilice el prefijo común `CX`.
5. Para introducir una descripción más larga, pulse el icono situado al lado del campo de descripción e introduzca una descripción en la ventana mostrada.
6. En Detalles, en la lista **Tipo de plantilla**, seleccione **Actividad**.
7. En Detalles, asigne un grupo propietario al procedimiento operativo estándar:
   a. Pulse el icono situado junto al campo **Grupo propietario**.
   b. En la ventana Seleccionar valor, pulse un valor de la lista para seleccionarlo.
8. Opcional: En **Duración**, especifique un límite de tiempo dentro del cual debe completarse el procedimiento operativo estándar . El formato para el límite de tiempo es *hh*`:`*mm*, donde *hh* es el número de horas y *mm* es el número de minutos. La fecha de vencimiento se calcula en función de la duración.
9. Añada tareas al procedimiento operativo estándar, según se requiera:
   a. Junto a la parte inferior derecha de la interfaz de usuario de Tivoli Service Request Manager, pulse **Fila nueva**. En Pasos de SOP, se añade una fila de tarea nueva a la lista de secuencia de tareas.
   b. Para **Secuencia**, y para **Tarea**, especifique el mismo número. Numere las tareas con el patrón siguiente: `10`, `20`, `30`, etc. Si utiliza este patrón, tendrá más flexibilidad para añadir y eliminar tareas más adelante.
   c. Para **Instrucción**, especifique una descripción de la tarea. Para seleccionar entre las descripciones que ha especificado anteriormente, pulse el icono situado junto al campo de descripción.
   d. Opcional: Asigne un flujo de trabajo:
      1) Para **Nombre de flujo de trabajo**, pulse el icono **Seleccionar valor**.

2) En la ventana **Seleccionar valor**, pulse un valor de la lista para seleccionarlo. Para reducir la lista, en el campo de filtro que se muestra en la parte superior de la lista, escriba las primeras letras del nombre de un flujo de trabajo que desee utilizar.
3) Expanda la fila de la tarea y, en Detalles, especifique más detalles, según sea necesario. Si lo desea, puede especificar un grupo de propietarios y valores de control de flujos. Si no especifica un grupo de propietarios y valores de control de flujos para la tarea, la tarea hereda los valores del procedimiento operativo estándar padre.

10. Para guardar el procedimiento operativo estándar, cerca de la parte superior de la interfaz de usuario de Tivoli Service Request Manager, pulse el icono **Guardar SOP**.
11. Para que se aplique el procedimiento operativo estándar a los sucesos especificados en la matriz de selección del procedimiento de operación estándar, asegúrese de cambiar el estado de `BORRADOR` a `ACTIVO`:
    a. Pulse el icono **Cambiar estado**.
    b. En la ventana Cambiar estado, desde la lista **Nuevo estado**, seleccione **Activo**.
    c. Opcional: Especifique valores para **A partir de la fecha** y **Memo**.
    d. Pulse **Aceptar**.
12. Para revisar los procedimientos de operación estándar disponibles, realice los pasos siguientes:
    a. Pulse la pestaña **Lista**.
    b. En Planes de trabajo de SOP, elija una de las opciones siguientes:
       - En el campo de filtro, pulse Intro para ver todos los procedimientos de operación estándar disponibles.
       - En el campo de filtro, especifique las primeras letras del nombre de un procedimiento operativo estándar.
    c. Para ver los detalles de un procedimiento operativo estándar, pulse el nombre de procedimiento operativo estándar en la lista. Los detalles se muestran en la pestaña **Procedimiento operativo estándar**.

Qué hacer a continuación

Si desea poder especificar el orden en que se ejecutan algunas o todas las actividades de un procedimiento operativo estándar, en Detalles, seleccione el recuadro de selección **¿Flujo controlado?**. Para obtener más información sobre cómo ordenar las actividades que se asignan a los usuarios o grupos basadas en procedimientos de operación estándar, consulte el Information Center de Maximo Asset Management y busque *control de flujo*.

En la matriz de selección del procedimiento de operación estándar, defina los parámetros de suceso que determinan para qué sucesos se selecciona el procedimiento operativo estándar.

Tareas relacionadas:

"Asignación de un usuario a grupo de personas" en la página 130
En un procedimiento operativo estándar, se pueden asignar tareas a grupos de personas predefinidos. Un usuario debe ser miembro de un grupo de personas particular para ver las tareas asignadas a grupo de personas.

Información relacionada:

Information Center de gestión de activos Maximo

Revisión de las entradas en la matriz de selección del procedimiento de operación estándar

En la matriz de selección del procedimiento de operación estándar, revise los criterios de selección para cada procedimiento operativo estándar. Los criterios de selección se basan en parámetros de suceso.

Procedimiento

1. Para abrir el portlet Procedimientos operativos estándar, en la interfaz de administración de WebSphere Portal, pulse **Intelligent Operations** > **Herramientas de personalización** > **Procedimientos operativos estándar**.
2. Para abrir la aplicación Matriz de selección de procedimiento operativo estándar, pulse **Matriz de selección de procedimiento operativo estándar**.
3. En la ventana Matriz de selección de procedimiento operativo estándar, para visualizar la fila de filtro, pulse el icono **Filtro**.
4. Determine qué campo de filtro se utilizará:
   - Categoría
   - Gravedad
   - Urgencia
   - Certeza
   - Nombre de SOP
5. Elija una de las opciones siguientes:
   - En el campo de filtro, pulse Intro para ver todas las entradas existentes relacionadas con el parámetro elegido o el nombre de procedimiento operativo estándar.
   - En el campo de filtro, especifique las primeras letras de un valor para filtrar.
   - Si está filtrando en un valor de parámetro, especifique los valores mediante la ventana Seleccionar valor:
     a. Junto al campo de filtro, pulse el icono **Seleccionar valor**.
     b. En la ventana Seleccionar valor, pulse un valor de la lista para seleccionarlo.
   - Para seleccionar el nombre de un procedimiento operativo estándar para filtrar mediante la ventana Procedimiento operativo estándar:
     a. Junto al campo de filtro **NOMBRE DE SOP**, pulse el icono **Menú Detalles** y, a continuación, pulse **Ir a procedimiento operativo estándar**.
     b. En la ventana Procedimiento operativo estándar, pulse la pestaña **Lista**.
     c. En Planes de trabajo de SOP, en el campo de filtro, especifique las primeras letras del nombre de un procedimiento operativo estándar.
     d. Para ver los detalles de un procedimiento operativo estándar, pulse el nombre de procedimiento operativo estándar en la lista. Los detalles se muestran en la pestaña **Procedimiento operativo estándar**.
     e. Para volver al nombre del procedimiento operativo estándar que se visualiza en la pestaña **Procedimiento operativo estándar**, en la esquina superior derecha, pulse **Regresar con valor**. El nombre de visualiza en el campo de filtro **Nombre de SOP** en la matriz de selección.
6. Para refinar adicionalmente la lista de entradas de criterios de selección mostrados, repita el Paso 5 utilizando uno de los campos de filtro listados en el Paso 4.

Definición de parámetros en la matriz de selección del procedimiento de operación estándar

En la matriz de selección del procedimiento de operación estándar, defina los parámetros de suceso que determinan si un procedimiento operativo estándar se selecciona para un suceso determinado.

Acerca de esta tarea

No puede guardar una matriz de selección del procedimiento de operación estándar que contenga dos filas de criterios de selección idénticas. Si procede, se muestra un mensaje de validación que le informa de que debe definir un conjunto de criterios de selección exclusivo para un procedimiento operativo estándar.

Procedimiento

1. Para abrir el portlet Procedimientos operativos estándar, en la interfaz de administración de WebSphere Portal, pulse **Intelligent Operations** > **Herramientas de personalización** > **Procedimientos operativos estándar**.
2. Para abrir la aplicación Matriz de selección de procedimiento operativo estándar, pulse **Matriz de selección de procedimiento operativo estándar**.
3. En la ventana Matriz de selección de procedimiento operativo estándar, para visualizar la fila de filtro, pulse el icono **Filtro**.
4. En la ventana **Matriz de selección de SOP**, en la esquina inferior derecha, pulse **Fila nueva**. Se añade una fila nueva a la matriz de selección.
5. Especifique valores para cada uno de los parámetros siguientes:
   - Categoría
   - Gravedad
   - Urgencia
   - Certeza

   Utilice una de las opciones siguientes para especificar valores para cada parámetro:
   - Para especificar valores mediante la ventana Seleccionar valor:
     a. Junto al campo de parámetro, pulse el icono **Seleccionar valor**.
     b. En la ventana Seleccionar valor, pulse un valor de la lista para seleccionarlo.
   - Para especificar el nombre del parámetro manualmente:
     a. Especifique las primeras letras del valor del parámetro en el campo.
     b. Pulse la tecla tabuladora para mover el cursor al siguiente campo y el valor del parámetro se completa automáticamente.
6. Para especificar el nombre del procedimiento operativo estándar en el campo **Nombre de SOP**, elija una de las siguientes opciones:
   - Para especificar el nombre del procedimiento operativo estándar mediante la ventana Procedimiento operativo estándar:
     a. Junto al campo **NOMBRE DE SOP**, pulse el icono **Menú Detalles** y, a continuación, pulse **Ir a procedimiento operativo estándar**.
     b. En la ventana Procedimiento operativo estándar, pulse la pestaña **Lista**.
     c. En Planes de trabajo de SOP, en el campo de filtro, especifique las primeras letras del nombre de un procedimiento operativo estándar.
     d. Para ver los detalles de un procedimiento operativo estándar, pulse el nombre de procedimiento operativo estándar en la lista. Los detalles se muestran en la pestaña **Procedimiento operativo estándar**.
     e. Para volver al nombre del procedimiento operativo estándar que se visualiza en la pestaña **Procedimiento operativo estándar**, en la esquina superior derecha, pulse **Regresar con valor**. El nombre se muestra en el campo **Nombre de SOP** de la fila nueva en la matriz de selección.
   - Especifique el nombre del procedimiento operativo estándar manualmente.
7. Pulse el icono **Guardar matriz**.

Gestión de recursos

Gestione los recursos en Tivoli Service Request Manager.

Sincronización de recursos de muestra en la base de datos IBM Intelligent Operations Center

Si quiere utilizar los recursos de muestra instalados con IBM Intelligent Operations Center, debe sincronizarlos con la base de datos de IBM Intelligent Operations Center manualmente.

Procedimiento

1. Inicie la sesión en Tivoli Service Request Manager Start Center como administrador.
2. Pulse **Ir a** > **Activos** > **Recursos de IOC (IntOpCtr)**.
3. Para ver todos los recursos de IBM Intelligent Operations Center de muestra, en la ventana Recursos (IntOpCtr) , de la pestaña **Lista** , pulse el campo **Recursos** y, a continuación, pulse Intro.
4. Para cada uno de los recursos que desea sincronizar con la base de datos de IBM Intelligent Operations Center , actualice el recurso. Por ejemplo, modifique la **Descripción** y guarde el cambio.
5. Verifique que los recursos sincronizados están listados en las siguientes tablas de base de datos de IBM Intelligent Operations Center :
   - `IOC.RESOURCE`
   - `IOC.RESOURCE_X_CAPABILITY`

Qué hacer a continuación

Si los recursos de muestra no se sincronizan correctamente en la base de datos de IBM Intelligent Operations Center, revise el archivo de registro de análisis de Tivoli Netcool/Impact. Entre el siguiente mandato:

```
tail –f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Revise también el archivo de registro de políticas de Tivoli Netcool/Impact en `/opt/IBM/netcool/impact/log/NCI_policylogger.log`. Para habilitar el archivo de registro de políticas de Tivoli Netcool/Impact, siga los pasos siguientes:

1. Inicie sesión en la consola administrativa de Tivoli Netcool/Impact en `http://`**`event_server`**`:9080/nci`.Inicie sesión como usuario `admin` con la contraseña `netcool`.
2. Pulse **Proyectos de IOC** .
3. En la pestaña **Servicios**, pulse **Registrador de políticas**.
4. Para **Registro de nivel superior**, cambie el valor de `0` a `3`.
5. Guarde los cambios.
6. Ejecute la prueba.

Para obtener más información acerca de la resolución de problemas de los archivos de registro, consulte el enlace al final del tema.

Conceptos relacionados:

"Archivos de registro de Servidor de sucesos" en la página 302
Utilice los procedimientos siguientes para habilitar rastreos y ver los registros para algunos de los sistemas de servidor de sucesos.

Creación o modificación de la categoría de sucesos a correlación de capacidades

Los recursos se muestran en el portlet Mapa dependiendo de la categoría del suceso seleccionado y de las prestaciones de recursos asignadas. Antes de crear un recurso, correlacione la capacidad del recurso con la categoría de suceso adecuada.

Antes de empezar

Para asegurarse de que las capacidades de recurso estén actualizadas, establezca el valor de la contraseña en el usuario administrativo de Tivoli Service Request Manager, por ejemplo, **`maxadmin`** a `maxadmin`.

Acerca de esta tarea

Al correlacionar una capacidad de recurso con una categoría de suceso se asegura de que, cuando visualice recursos cercanos en el portlet de IBM Intelligent Operations Center Detalles, se muestren los recursos apropiados en el portlet de Mapa. Por ejemplo, si visualiza recursos cercanos para la categoría

meteorológica de un suceso, se mostrará un almacén que contiene sacos de arena, donde el almacén es el tipo de recurso y los sacos de arena son una capacidad correlacionada del almacén.

Procedimiento

1. Inicie la sesión en Tivoli Service Request Manager Start Center como administrador.
2. Pulse **Ir a** > **Configuración del sistema** > **Configuración de plataforma** > **Dominios**.
3. Seleccione la opción adecuada:
   - Para crear una categoría de sucesos para la correlación de capacidades, pulse **Nueva fila** e introduzca la información adecuada en los campos.
   - Para modificar una categoría de sucesos existente para la correlación de capacidades, utilice el campo de filtro para mostrar las correlaciones de categoría de sucesos adecuada y pulse la fila cuya información desea editar y modificar.
   - Para suprimir una categoría de sucesos existente para la correlación de capacidades, utilice el campo de filtro para mostrar las correlaciones de categoría de sucesos adecuadas y, a continuación, pulse el icono **Marcar fila para supresión** al final de la fila que desea suprimir.
4. Pulse el icono **Guardar dominio** .
5. Verifique que los recursos correlacionados se listen en las tablas de base de datos IBM Intelligent Operations Center siguientes:
   - `IOC.RESOURCE`
   - `IOC.RESOURCE_X_CAPABILITY`

Resultados

Los nuevos recursos cuya capacidad se correlaciona con la categoría de suceso del suceso seleccionado actualmente se muestra en el portlet de IBM Intelligent Operations Center Mapa inmediatamente. Los recursos actualizados cuyas posibilidades se correlacionan con la categoría de suceso del suceso seleccionado actualmente se muestran sólo después de que la página que contiene el portlet de IBM Intelligent Operations CenterMapa se vuelve a cargar.

Qué hacer a continuación

- Si los recursos correlacionados no se listan correctamente en la base de datos de IBM Intelligent Operations Center, revise el archivo de registro de Tivoli Netcool/Impact. Entre el siguiente mandato:

  ```
  tail –f /opt/IBM/netcool/omnibus/log/ioc_xml.log
  ```

  Para obtener más información acerca de la resolución de problemas de los archivos de registro, consulte el enlace al final del tema.
- Si desea correlacionar más de dos categorías de sucesos con una capacidad, utilice un mandato de DB2 para realizar la correlación. Siga estos pasos:
  1. Para iniciar sesión en servidor de datos como usuario de base de datosTivoli Service Request Manager , entre el siguiente mandato: `su - db2inst6`
  2. Para conectarse a la base de datos IBM Intelligent Operations Center , entre el siguiente mandato: `db2 connect to maximo`
  3. Para correlacionar una categoría de suceso con una capacidad, introduzca el mandato siguiente:

     ```
     insertar en synonymdomain
     los valores(domainid, maxvalue, value, description, defaults, synonymdomainid, valueid)
     ('PLUSICATCPLMAP', 'category_name', 'capability_name',
     'mapping_description', 0,   NEXTVAL FOR synonymdomainseq,
     'PLUSICATCPLMAP|mapping_key');
     ```

     En el mandato anterior, sustituya las variables *category_name*, *capability_name*, *mapping_description* y *mapping_key* por valores adecuados. Para *mapping_key*, cree un valor adecuado. Por ejemplo, el mandato siguiente correlaciona la categoría de suceso `Met` con la capacidad `COT` y asigna el valor `METCOT` con *clave_correlación*.

```
insertar en synonymdomain
los valores(domainid, maxvalue, value, description, defaults, synonymdomainid, valueid)
('PLUSICATCPLMAP', 'Met', 'COT', 'Has cots', 0,   NEXTVAL FOR synonymdomainseq,
'PLUSICATCPLMAP|METCOT');
```

4. Para completar la escritura para la base de datos, entre el siguiente mandato: `db2 commit;`

Creación de un recurso

Cree un recurso en la interfaz de usuario de Tivoli Service Request Manager .

Antes de empezar

Asegúrese de que la capacidad del nuevo recurso está asignada a una categoría de manera que los recursos se muestran en el portletMapa en la interfaz de usuario de IBM Intelligent Operations Center .

Procedimiento

1. Inicie la sesión en Tivoli Service Request Manager Start Center como administrador.
2. Pulse **Ir a** > **Activos** > **Recursos (IntOpCtr)**.
3. En la ventana Recursos de IOC , pulse el icono **Nuevo recurso** .
4. En la pestaña **Recurso** , entre los siguientes detalles:

   Recurso
   Un identificador exclusivo para el recurso.

   Descripción larga
   El nombre del recurso que se muestra en la interfaz de usuario de IBM Intelligent Operations Center , en el portlet Detalles , en la pestaña **Recursos** .

   Descripción breve
   Una descripción breve del recurso que se muestra como ayuda contextual si pasa el ratón por encima del recurso en el portlet Mapa de la interfaz de usuario de IBM Intelligent Operations Center .

   Latitud
   Posición latitudinal de la ubicación del recurso.

   Longitud
   Posición longitudinal de la ubicación del recurso.
5. Pulse la pestaña **Capacidades**.
6. Al lado del campo **Clasificación** , pulse el icono **Menú de detalles** y, a continuación, pulse **Clasificar**.
7. En la ventana Clasificar , vaya al árbol de navegación para ubicar la clasificación de recurso adecuada.
8. Pulse un nombre de clasificación; por ejemplo, un almacén. Se muestra una tabla de prestaciones asociada con la clasificación en la ventana Recursos de IOC .
9. En la tabla Prestaciones, pulse las prestaciones adecuadas y entre el **Valor numérico**.
10. Pulse el icono **Guardar recurso** .

Qué hacer a continuación

Verifique que el recurso está listado en las siguientes tablas de base de datos deIBM Intelligent Operations Center :

- `IOC.RESOURCE`
- `IOC.RESOURCE_X_CAPABILITY`

Tareas relacionadas:

"Creación o modificación de la categoría de sucesos a correlación de capacidades" en la página 137
Los recursos se muestran en el portlet Mapa dependiendo de la categoría del suceso seleccionado y de las prestaciones de recursos asignadas. Antes de crear un recurso, correlacione la capacidad del recurso con la categoría de suceso adecuada.

Visualización, actualización o supresión de un recurso

Acceda a la interfaz de usuario de Tivoli Service Request Manager a través de la interfaz de usuario de IBM Intelligent Operations Center y visualice, actualice o suprima los recursos.

Acerca de esta tarea

El siguiente procedimiento describe cómo acceder a los datos de recurso en Tivoli Service Request Manager a través de la interfaz de usuario de IBM Intelligent Operations Center . Para acceder a los datos de recurso directamente a través de Tivoli Service Request Manager, utilice los pasos siguientes:

1. Inicie sesión en Tivoli Service Request Manager Start Center.
2. Pulse **Ir a** > **Activos** > **Recursos (IntOpCtr)**.
3. Para instalar todos los recursos de IBM Intelligent Operations Center , en la ventana Recursos (IntOpCtr) , en la pestaña **Lista** , pulse en el campo **Recursos** y, después, la tecla Intro.
4. En la lista, pulse la fila para el recurso que desea modificar.
5. Pulse la pestaña **Recurso** o la pestaña **Prestaciones** , según sea necesario.

Procedimiento

1. Abra la interfaz de usuario de IBM Intelligent Operations Center.
2. En el portlet Detalles , en la pestaña **Sucesos e incidencias** , identifique un suceso en la lista cuyos recursos desea visualizar, actualizar o suprimir.
3. Para ver una lista de los recursos en las proximidades del suceso, pulse con el botón derecho del ratón en el suceso y, después, pulse **Ver recursos de la zona** y seleccione el radio del área en el que desea centrarse. Se muestra una lista de recursos en la pestaña **Recursos**.
4. En la pestaña **Recursos** , pulse con el botón derecho del ratón sobre una fila de la lista de recursos y seleccione una opción del menú:
   - Para actualizar la información sobre un recurso, haga clic en **Actualizar**.
   - Para eliminar un recurso de la lista y el mapa, pulse **Suprimir**.
   - Para ver la información acerca de un recurso, pulse **Propiedades**.

   Cualquiera que sea la opción que elija, se muestra el recurso en Tivoli Service Request Manager, en la pestaña**Recurso** .
5. En Tivoli Service Request Manager, en la pestaña **Recursos**, puede optar por realizar las siguientes acciones en el recurso:
   - Actualizar el nombre de recurso, descripciones, latitud y longitud.
   - Para suprimir el recurso, seleccione **Suprimir recurso** de la lista **Seleccionar acción** .
6. En la pestaña **Capacidades**, puede optar por realizar las siguientes acciones en las capacidades del recurso.
   - Pulse las prestaciones adecuadas y modifique el **Valor numérico**. Para correlacionar una capacidad con el recurso, el valor debe ser 1 o más.
   - Seleccione una prestación y, a continuación, pulse el icono **Marcar fila a suprimir** al final de la fila.
7. Cuando termine de actualizar el recurso, pulse el icono **Guardar recurso** .

Qué hacer a continuación

Para poder ver los datos de recurso actualizados en la interfaz de usuario deIBM Intelligent Operations Center , restablezca Mapa. A continuación, revise los recursos para el suceso a través del portlet Detalles .

Creación de un tipo de recurso

Cree un tipo de recurso en Tivoli Service Request Manager.

Acerca de esta tarea

Puede definir una jerarquía de tipos de recurso, de manera que los tipos de recurso tengan tipos de recurso hijos, etc.

Procedimiento

1. Inicie la sesión en Tivoli Service Request Manager Start Center como administrador.
2. Pulse **Ir a** > **Administración** > **Clasificaciones**.
3. Para ver todos los tipos de recurso de IBM Intelligent Operations Center existentes, en la pestaña **Lista**, del campo **Descripción**, introduzca `RESOURCE`. Se muestran todos los tipos de recurso de la jerarquía.
4. Pulse el tipo de recurso o el tipo de recurso hijo para el que desee crear un tipo de recurso hijo. Los detalles de clasificación del padre del nuevo tipo de recurso se muestran en la pestaña **Clasificaciones**.
5. En la pestaña **Clasificaciones**, en Hijos, pulse **Fila nueva**.
6. En la fila vacía que se ha añadido a la lista, introduzca los valores siguientes para el nuevo tipo de recurso:
   a. En la columna **Clasificación**, introduzca un nombre.
   b. En la columna Descripción de la clasificación, introduzca una descripción.
   c. Para imperdir que el nombre del tipo de recurso se cambie al guardar el tipo de recurso, borre la casilla de verificación **Generar descripción**.
7. Pulse el icono **Guardar clasificación** .
8. Para añadir un icono gráfico para el nuevo tipo de recurso, lleve a cabo los subpasos siguientes:
   a. Guarde copias del gráfico en dos tamaños en formato PNG. El icono gráfico más grande se muestra en el portlet de Mapa y el icono gráfico más pequeño se muestra en la lista de sucesos en el portlet de Detalles.

      Tamaño 24 píxeles x 24 píxeles
      Por ejemplo, *nuevo_recurso*_24.png

      Tamaño 16 x 16 píxeles
      Por ejemplo, *nuevo_recurso*_16.png
   b. Copie todos los archivos PNG en el directorio adecuado en servidor de aplicaciones:
      - `/opt/IBM/WebSphere/wp_profile/installedApps/ICPWPSNode/iss_portal_ear.ear/iss_common_widgets_web.war/images/resource_icons/PNG-24x24/Normal_State`
      - `/opt/IBM/WebSphere/wp_profile/installedApps/ICPWPSNode/iss_portal_ear.ear/iss_common_widgets_web.war/images/resource_icons/PNG-16x16/Normal_State`
   c. Compruebe que los iconos se muestren correctamente en el enlace del navegador web correspondiente:
      - http://**appserver**/ibm/iss/common/widgets/images/resource_icons/PNG-24x24/Normal_State/new_resource_24.png
      - http://**appserver**/ibm/iss/common/widgets/images/resource_icons/PNG-16x16/Normal_State/new_resource_16.png

Agregar una capacidad a un tipo de recurso

Cree una capacidad en Tivoli Service Request Manager.

Procedimiento

1. Inicie la sesión en Tivoli Service Request Manager Start Center como administrador.
2. Pulse **Ir a** > **Administración** > **Clasificaciones**.
3. Para ver todas las clasificaciones de recursos de IBM Intelligent Operations Center existentes, en la pestaña **Lista** , filtre por RESOURCE.
4. Pulse la pestaña **Clasificaciones** .
5. En Hijos, en la lista, pulse el tipo de recurso para el que desea añadir una capacidad.
6. Para evitar que el nombre de recurso se cambie cuando guarde la clasificación, borre la casilla **Generar descripción**.
7. En Atributos, pulse **Fila nueva**.
8. Introduzca la información de la nueva capacidad:
   a. Para **Atributo**, introduzca un nombre.
   b. En el campo de la derecha del campo **Atributo**, introduzca una descripción.
   c. Para entrar un valor para **Tipo de datos**, pulse el icono Seleccionar valor y elija un valor en la ventana Seleccionar valor .
   d. Para especificar que los recursos hijo hereden esta capacidad, seleccione **Aplicar jerarquía hacia abajo**.
9. Pulse el icono **Guardar clasificación** .

procedimientos de operación estándar, flujos de trabajo de muestra y recursos

El procedimientos de operación estándar, flujos de trabajo de muestra y los recursos se proporcionan cuando instala IBM Intelligent Operations Center versión 1.5.

Procedimientos de operación estándar

A continuación, se muestran los tres procedimientos de operación estándar que se proporcionan:

PLUSIMITIG: Preparación inicial para el mal tiempo (Mitigar)

PLUSIMITIG contiene los siguientes pasos:

1. Valide la gravedad del tiempo. Paso manual sin flujos de trabajo asociado.
2. Aumente la puntuación de gravedad si es necesario. Paso manual sin flujos de trabajo asociado.

PLUSIPREPA: Prepárese para la evacuación por mal tiempo (Preparar)

PLUSIPREPA contiene los siguientes pasos:

1. Prepare los refugios de evacuación. Paso manual con flujo de trabajo PLUSISOP00 asociado.
2. Identifique los recursos de ayuda de evacuación. Paso manual con flujo de trabajo PLUSISOP00 asociado.
3. Evalúe la disponibilidad de los recursos de ayuda. Paso manual con flujo de trabajo PLUSISOP00 asociado.

PLUSIRESPO: Evacuar áreas afectadas (Responder y recuperar)

PLUSIRESPO contiene los siguientes pasos:

1. Aprobar la directiva de evacuación. Paso manual sin flujos de trabajo asociado.
2. Asegúrese de que las rutas de salida están libres. Paso manual sin flujos de trabajo asociado.

El matriz de selección del procedimiento de operación estándar está lleno con datos que desencadenan la selección de los tres procedimientos de operación estándar, como vemos en la tabla siguiente:

Tabla 35. Datos de ejemplo de Matriz de selección del procedimiento de operación estándar

Categoría	Gravedad	Urgencia	Certeza	Nombre de Procedimiento operativo estándar
Cumplido	Grave	Futuro	Observado	PLUSIMITIG
Cumplido	Grave	Futuro	Probablemente	PLUSIMITIG
Cumplido	Extremo	Futuro	Observado	PLUSIPREPA
Cumplido	Extremo	Futuro	Probablemente	PLUSIPREPA
Cumplido	Extremo	Inmediato	Observado	PLUSIRESPO

Ejemplo de flujo de trabajo

Hay un flujo de trabajo de ejemplo:

PLUSISOP00: Complete la acción de actividad
PLUSISOP00 flujo de trabajo desencadena una acción para cambiar el estado de una actividad en `COMP` (completa).

El PLUSISOP00 flujo de trabajo está asociado con cada uno de los pasos del ejemplo de PLUSIPREPA procedimiento operativo estándar. Si inicia uno de los pasos, el estado del paso se marca automáticamente como completo.

Recursos de muestra

La tabla siguiente lista los recursos de muestra, que se proporcionan en el dominio `PLUSICATCPLMAP` :

Tabla 36. Recursos de muestra

Recurso	Descripción	Tipo de recurso
BASCOMEYE	Bascombe Eye Institute	RESOURCES\HOSPITAL
BLUEFISHW	Blue Fish Warehouse	RESOURCES\WAREHOUSE
DOCTORSH	Doctor's Hospital	RESOURCES\HOSPITAL
MERYCYH	Mercy Hospital	RESOURCES\HOSPITAL
MAMICHILD	Miami Children's Hospital	RESOURCES\HOSPITAL
SFFOODDIST	South Florida Food Distribution	RESOURCES\WAREHOUSE
TTLEASING	Tropical Trailer Leasing Corporation	RESOURCES\WAREHOUSE
UNIMIAMI	University of Miami Hospital	RESOURCES\HOSPITAL
WTDCDIST	WTDC Distribution Center Miami	RESOURCES\WAREHOUSE

Capítulo 5. Personalización de la solución

La personalización de la solución para que se ajuste a su funcionamiento concreto incluye tareas descritas en esta sección en relación a la interfaz de usuario y a la tabla de propiedades del sistema. La personalización está muy relacionada con la intergración de la solución y los enlaces apropiados están incluidos en los temas del indicador clave de rendimiento (KPI) y de suceso de esta sección.

Personalización de la interfaz de usuario

Puede personalizar los elementos de la interfaz de usuario IBM Intelligent Operations Center para que se adapten a su funcionamiento

Además de la personalización del diseño y la apariencia de los portlets, también puede crear nuevas páginas. Para obtener más información, consulte la documentación del producto WebSphere Portal .

Información relacionada:

 Documentación del producto IBM WebSphere Portal 7

Ubicación de la interfaz de usuario

Los valores de navegador determinan el idioma y los valores de fecha y hora para la interfaz de usuario de IBM Intelligent Operations Center . Un administrador puede personalizar los formatos de fecha y hora.

En IBM Intelligent Operations Center, los valores del navegador determinan el idioma del texto. Donde no está disponible ese idioma en IBM Intelligent Operations Center, se utiliza la relación más cercana; por ejemplo, el francés canadiense revierte al francés que a su vez revierte al inglés que siempre está disponible. La configuración del navegador también determina el huso horario para todas las horas y fechas que se muestran. La fecha y hora deIBM Intelligent Operations Center se ajusta automáticamente al huso horario del navegador.

Todas las fechas y horas se presentan en su zona horaria en el formato especificado en la tabla de base de datos de propiedades del sistema. Las propiedades del sistema contienen la cadena de formato de fecha y hora. Para cambiar el valor en la base de datos editando la propiedad, siga el enlace al final del tema.

Conceptos relacionados:

"Especificación de datos de configuración de todo el sistema" en la página 182
La tabla de propiedades del sistema IBM Intelligent Operations Center almacena datos de configuración IBM Intelligent Operations Center .

"Utilización del PAC para sucesos de ICR" en la página 100
El WebSphere Message Broker, que se proporciona como parte de IBM Intelligent Operations Center, acepta mensajes de suceso CAP y utiliza los datos en los cálculos del indicador clave de rendimiento (KPI) .

Lista de portlets

IBM Intelligent Operations Center es una solución basada en portlet que utiliza la tecnología de portal para proporcionar herramientas y la información de pantalla. Todos los portlets incluidos en IBM Intelligent Operations Center se enumeran en las secciones siguientes.

Portlets de usuario

La tabla siguiente lista los portlet de usuario incluidos en IBM Intelligent Operations Center. La página también indica en qué vistas de página de muestra está disponible cada portlet.

Puede personalizar los portlets. Para obtener más información, consulte el enlace al final del tema.

Tabla 37. Portlets de usuario en IBM Intelligent Operations Center

Portlet	Descripción	Vistas de página de muestra
"Contactos" en la página 277	El portlet Contactos puede mostrar una lista de contactos organizados por categoría. Puede organizarlas los contactos en categorías basadas en las personas con las que tiene que comunicarse. Por ejemplo, puede tener una categoría para contactos de trabajo generales y otra categoría para contactos de trabajo de un proyecto concreto. Con el portlet Contactos, puede comunicarse con la gente y modificar su estado en línea, sus contactos o sus grupos.	• "Vista Supervisor: Estado" en la página 273 • "Vista Supervisor: Operaciones" en la página 274 • "Vista Operador: Operaciones" en la página 275
"Detalles" en la página 278	El portlet Detalles es un portlet de lista interactivo. Todos los sucesos que está autorizado a ver son visibles en la lista de sucesos y en cualquier portlet de mapa vinculado al portlet Detalles.	• "Vista Supervisor: Operaciones" en la página 274 • "Vista Operador: Operaciones" en la página 275 • "Vista Mapa de ubicación" en la página 276
"Obtención de detalles de indicador clave de rendimiento" en la página 281	Para centrarse en un categoría de ICR específica en el portlet Obtención de detalles de indicador clave de rendimiento, haga clic en la categoría en el portlet Estado. Luego esta categoría se muestra en solitario en el portlet Obtención de detalles de indicador clave de rendimiento. Puede utilizar la lista para inspeccionar los ICR subyacentes hasta llegar a los detalles del ICR que causara el cambio de estado.	• "Vista Supervisor: Estado" en la página 273
"Mapa de ubicación" en la página 282	Utilice el Mapa de ubicación portlet para ver los sucesos marcados en un mapa de ubicación. Un mapa de ubicación en IBM Intelligent Operations Center es un mapa o plano con zonas predefinidas para la interacción, por ejemplo, los asientos en un estadio deportivo.	• "Vista Mapa de ubicación" en la página 276

Tabla 37. Portlets de usuario en IBM Intelligent Operations Center (continuación)

Portlet	Descripción	Vistas de página de muestra
"Mapa" en la página 285	En el portlet Mapa : Un mapa de la región geográfica con marcadores de sucesos y recursos. Un formulario de filtro para seleccionar las categorías de los sucesos que se muestran en el mapa y en los portlets enlazados con el portlet Mapa. Un formulario de filtro para seleccionar las prestaciones de los recurso que se muestran en el mapa y en la pestaña **Recursos**, en el portlet Detalles enlazado. Para ver este formulario, seleccione primero **Ver recursos de la zona** en el portlet Detalles .	• "Vista Supervisor: Operaciones" en la página 274 • "Vista Operador: Operaciones" en la página 275
"Mis actividades" en la página 290	Un usuario que haya iniciado sesión puede ver las actividades asignadas a ellos en el portlet Mis actividades. En el portlet Mis actividades, las actividades se agrupan por sus procedimientos de operación estándar de nivel superior. Cada procedimiento operativo estándar se corresponde con un suceso individual.	• "Vista Supervisor: Estado" en la página 273 • "Vista Supervisor: Operaciones" en la página 274 • "Vista Operador: Operaciones" en la página 275
"Notificaciones" en la página 293	El portlet Notificaciones proporciona una lista dinámica e interactiva de las alertas que resultan de cambios en ICR y sucesos relacionados. El papel de este portlet es llamar la atención sobre los cambios en ICR o en estado de sucesos. La lista contiene detalles clave de cada una de las alertas.	• "Vista Supervisor: Estado" en la página 273 • "Vista Supervisor: Operaciones" en la página 274 • "Vista Operador: Operaciones" en la página 275
"Informes " en la página 294	Utilice el portlet Informes para ver un informe de sucesos como gráfico. El portlet proporciona varias opciones para agrupar suceso y puede elegir sucesos por un rango de fechas o por una fecha concreta. Estos informes le ayudan a planificar respuestas para sucesos actuales o futuros.	• "Supervisor: informes " en la página 276 • "Operador: informes" en la página 276
"Estado" en la página 297	El portlet Estado proporciona un resumen de nivel ejecutivo del estado de los ICR en las organizaciones que tienen permiso para ver. Utilice este portlet para ver cambios actualizados en el estado de ICR para poder planificar y tomar medidas si es necesario.	• "Vista Supervisor: Estado" en la página 273

Tareas relacionadas:

"Personalización de portlets" en la página 149
Como administrador, puede cambiar los valores de portlet para personalizarlo.

Portlets administrativos

La siguiente tabla lista los portlets administrativos incluidos en IBM Intelligent Operations Center. Los portlets administrativos están en la página Administración.

Tabla 38. Portlets administrativos en IBM Intelligent Operations Center

Portlet	Descripción
"Acerca de" en la página 199	Utilice el portlet Acerca de para ver detalles de la versión del IBM Intelligent Operations Center y el IBM Smarter Cities Software Solutions integrado que ha instalado. También puede ver detalles de las actualizaciones que aplicó desde la instalación.
"Consolas de administración" en la página 207	Utilice el portlet Consolas de administración para administrar los servicios proporcionados por la solución.
"Verificación de componentes" en la página 214	La herramienta Comprobación de verificación del sistema prueba componentes dentro de IBM Intelligent Operations Center para determinar si son accesibles y operativos.
"Resumen de permisos de usuario" en la página 83	El portlet Resumen de permisos de usuario visualiza detalles sobre pertenencia a grupos y permisos otorgados a los usuarios.
"Indicadores clave de rendimiento" en la página 173	En el portlet Indicadores clave de rendimiento puede ver, cambiar, copiar, crear y suprimir KPI. También puede personalizar las jerarquías de ICR que aparecen en los portlets Estado y Obtención de detalles de indicador clave de rendimiento.
"Gestor de mapas de ubicación" en la página 181	Utilice el portlet Gestor de mapas de ubicación para personalizar el portletMapa de ubicación .
"Procedimientos operativos estándar" en la página 131	Puede definir procedimientos de operación estándar y actividades para gestionar sucesos que vienen con IBM Intelligent Operations Center. Utilice el portlet Procedimientos operativos estándar para acceder a las aplicaciones procedimiento operativo estándar, matriz de selección del procedimiento de operación estándar y diseñador del flujo de trabajo en Tivoli Service Request Manager.
"Script de suceso" en la página 111	Utilice el portlet Script de suceso para escribir un script para crear una lista secuencial de sucesos que se van a publicar a intervalos de tiempo predefinidos.
"Ejemplo de aplicación de publicación" en la página 107	El portlet Ejemplo de aplicación de publicación es una herramienta de pruebas automatizada diseñada para la gestión del administrador o la verificación de una solución. Un administrador puede utilizar el portletEjemplo de aplicación de publicación como aplicación cliente para probar la publicación de mensajes CAP en IBM Intelligent Operations Center. El portlet Ejemplo de aplicación de publicación puede eliminar el requisito para crear manualmente una aplicación cliente de prueba.

Tareas relacionadas:

"Personalización de portlets"
Como administrador, puede cambiar los valores de portlet para personalizarlo.

Creación o personalización de una página

Para crear páginas nuevas que se incluyan en IBM Intelligent Operations Center y especificar qué portlets mostrar en esas páginas. Puede personalizar la apariencia y el diseño de los portlets incluidos en cada página.

Acerca de esta tarea

Utilice la interfaz de usuario de WebSphere Portal para personalizar páginas y portlets.

Nota: Al crear o editar el diseño de una página, asegúrese de que los portlets operan correctamente y siguen las reglas siguientes:

- Los portlets Mapa y Detalles deben estar en el mismo grupo y en la misma página para permitir la adición de un evento desde el portlet Mapa.
- Los portlets Mis actividades y Detalles deben estar en el mismo grupo y en la misma página para permitir la solicitud de detalles sobre un evento desde el portlet Mis actividades o la solicitud de detalles de un Procedimiento operativo estándar desde el portlet Detalles.

Procedimiento

1. Para abrir WebSphere Portal, pulse la pestaña **Administración** .
2. En WebSphere Portal, pulse **Interfaz de usuario del portal**.
3. Pulse la opción necesaria:
   - Para trabajar con las páginas o crear páginas nuevas, pulse **Gestionar páginas**.
   - Para registrar temas y skins, establezca el tema predeterminado y el skin predeterminado para cada tema, pulse **Temas y Skins**.
   - Para personalizar los elementos de sitio clave en temas, incluyendo el banner, navegación, fuentes y colores, pulse **Personalizador de temas**.
4. Realizar modificaciones necesarias. Para obtener más información acerca del uso de WebSphere Portal para personalizar portlets, consulte el enlace en la parte inferior del tema para la documentación del producto de WebSphere Portal .

Información relacionada:

Documentación del producto IBM WebSphere Portal 7

Personalización de portlets

Como administrador, puede cambiar los valores de portlet para personalizarlo.

Acerca de esta tarea

Hay dos modos posibles de personalización, y ambos cambian los valores de portlet para todos los usuarios:

- **Editar valores compartidos** cambia el portlet únicamente para la instancia de dicho portlet en la que se encuentre cuando cambie los valores.
- **Configurar** cambia los valores globales del portlet para todas las instancias de dicho portlet, allí donde dichas instancias aparezcan.

Los modos de personalización que están disponibles dependen de los permisos asociados con el ID de usuario. Los valores globales son reemplazados por los valores compartidos.

Procedimiento

1. Inicie sesión en el portal de la solución como administrador.
2. Pulse en la esquina superior derecha del portlet para ver el menú del portlet.
3. Pulse **Editar valores compartidos**, o **Configurar**.
4. Entre los valores en los campos proporcionados.
5. Para cerrar la ventana de configuración, pulse uno de los botones:
   - **Guardar** para guardar cambios.
   - **Cancelar** para cancelar cambios.
   - **Restaurar valores predeterminados** para volver a la configuración global predeterminada.

Resultados

Cualquier valor que haya guardado tendrá efecto la próxima vez que se renueve el portlet. Los valores de configuración global predeterminados proporcionados con IBM Intelligent Operations Center los utilizan parámetros que no se han restablecido.

Valores del portlet Acerca de

Personalice el portlet Acerca de cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet Acerca de . Los parámetros de personalización se describen en la siguiente tabla.

Tabla 39. Parámetros de personalización del portlet Acerca de

Parámetro	Descripción	Valor predeterminado
Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`400`
Altura máxima del portlet	Número de píxeles que indica la altura máxima del portlet.	`600`

Conceptos relacionados:

"Acerca de" en la página 199
Utilice el portlet Acerca de para ver detalles de la versión del IBM Intelligent Operations Center y el IBM Smarter Cities Software Solutions integrado que ha instalado. También puede ver detalles de las actualizaciones que aplicó desde la instalación.

Valores del portlet Consolas de administración

Personalice el portlet Consolas de administración cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet Consolas de administración . Los parámetros de personalización se describen en la siguiente tabla.

Tabla 40. Parámetros de personalización del portlet Consolas de administración

Parámetro	Descripción	Valor predeterminado
JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`AdministrationConsolePortletHelp`

Tabla 40. Parámetros de personalización del portlet Consolas de administración (continuación)

Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`400`
Altura máxima del portlet	Número de píxeles que indica la altura máxima del portlet.	`450`
Título del portlet	Título para sustituir el título que se proporciona con la solución.	Si no introduce un valor para este parámetro, se mostrará el título proporcionado por la solución, es decir Consolas de administración.
Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica ningún paquete de recursos, no se busca ninguna clave y el título se muestra como proporcionado por la solución.	No hay paquete de recursos predeterminado.

Conceptos relacionados:

"Consolas de administración" en la página 207
Utilice el portlet Consolas de administración para administrar los servicios proporcionados por la solución.

Valores del portlet Contactos

Personalice el portlet Contactos cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet Contactos . Los parámetros de personalización se describen en la siguiente tabla.

Tabla 41. Parámetros de personalización del portlet Contactos

Parámetro	Descripción	Valor predeterminado
JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`SametimeWebClientPortletHelp`
Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`250`
Altura máxima del portlet	Número de píxeles que indica la altura máxima del portlet.	`600`
Título del portlet	Título para sustituir el título que se proporciona con la solución.	Si no se introduce un valor para este parámetro, el título suministrado por la solución que se muestra es el siguiente: Contactos.
Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica ningún paquete de recursos, no se busca ninguna clave y el título se muestra como proporcionado por la solución.	No hay paquete de recursos predeterminado.

Conceptos relacionados:

"Contactos" en la página 277
Utilice el portlet Contactos para enviar mensajes instantáneos dentro de la solución.

Valores del portlet Detalles

Personalice el portlet Detalles cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet Detalles . Los parámetros de personalización se describen en la siguiente tabla.

Tabla 42. Los parámetros de personalización para el Detalles portlet

Nombre de parámetro	Descripción	Valor predeterminado
Columnas	Especificaciones y orden de columnas que visualizar en la lista.	`[{"id": "commonevents.headline", "width": "20"}, {"id": "commonevents.eventType", "width": "7"}, {"id": "commonevents.category", "width": "10"}, {"id": "commonevents.severity", "width": "10"}, {"id": "commonevents.certainty", "width": "10"}, {"id": "commonevents.urgency", "width": "10"}, {"id": "commonevents.sent", "width": "12", "sortPriority": "1", "sortAscending": "false"}]`
Condiciones	Condiciones adicionales para la visualización de sucesos o recursos; las condiciones adicionales no se pueden alterar utilizando la barra de herramientas o el filtro de mapa. El valor predeterminado es que no se aplican condiciones adicionales.	`[]`
JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`CommonEventsPortletHelp`
Ocultar añadir suceso	Valor True o False para ocultar o mostrar el botón **Añadir sucesos** y la opción de menú emergente.	`true`
Ocultar añadir recurso	Valor verdadero o falso para ocultar o mostrar el botón **Añadir recursos** en la pestaña **Recursos**.	`true`
Ocultar sucesos	Valor verdadero o falso para ocultar o mostrar la pestaña **Sucesos e incidentes** .	`false`
Ocultar recursos	Valor verdadero o falso para ocultar o mostrar la pestaña **Recursos** .	`false`
Ocultar barra de herramientas	Valor verdadero o falso para ocultar o mostrar la barra de herramientas en la parte superior de la lista.	`true`

Tabla 42. Los parámetros de personalización para el Detalles portlet (continuación)

Ignorar modalidad cancelar recurso	True o false para reconocer o ignorar el mensaje de cancelación de modo de recurso entrante desde el portlet de Mapa.	`false`
Ignorar creación de sucesos	Valor true o false para reconocer o ignorar sucesos que creó el usuario en el portlet Mapa .	`false`
Ignorar los cambios del filtro de sucesos	Valor true o false para reconocer o ignorar las selecciones del filtro de sucesos que realiza el usuario en el portlet Mapa .	`false`
Ignorar selección de sucesos	Valor true o false para reconocer o ignorar la selección de sucesos de entrada realizada por el usuario en el portlet Mapa .	`false`
Ignorar tareas de sucesos	Valor verdadero o falso para reconocer o ignorar todas las selecciones de menú emergente de los sucesos.	`false`
Ignorar restablecer correlación	Valor true o false para reconocer o ignorar un clic del botón **Recursos** en el portlet.	`false`
Ignorar filtro de recursos cambiado	Valor verdadero o falso para reconocer o ignorar las selecciones del filtro de recursos realizadas por el usuario en el portlet Mapa .	`false`
Ignorar tareas de recursos	Valor true o fase para reconocer o ignorar todas las selecciones de menú emergente de los recursos.	`false`
Identificador de grupo del portlet	Nombre del grupo al que pertenece este portlet. Un nombre común configura la comunicación entre los portlets Mapa, Detalles y Mapa de ubicación en la misma página.	`valor predeterminado`
Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`350`
Altura máxima del portlet	Número de píxeles que indica la altura máxima del portlet.	`600`
Título del portlet	Título para sustituir el título que se proporciona con la solución.	Si no se introduce un valor para este parámetro, el título suministrado por la solución que se muestra es el siguiente: Detalles.
Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica ningún paquete de recursos, no se busca ninguna clave y el título se muestra como proporcionado por la solución.	No hay paquete de recursos predeterminado.

Nota: La explicación de lo que ocurre con el título del portlet cuando se proporciona un paquete de recursos se aplica también al título de la columna que tiene su origen en el mismo paquete de recursos.

Parámetro Columnas

El valor del parámetro **Columnas** está en una matriz de objetos JSON que se puede configurar como se explica en Tabla 43.

Tabla 43. Objetos dentro del valor de parámetro Columnas del portlet Detalles

Objeto	Contiene
`id`	identificador de columna para indicar que se va a mostrar la columna
`width`	Número de píxeles que indica el ancho de columna
`format`	Cadena que representa el formato que se utilizará para las columnas de fecha y hora, la entrada sobrescribe el valor de la tabla `sysprop`
`sortAscending`	• Valor `true` para utilizar en orden de clasificación ascendente en los elementos de columna • Valor `false` para utilizar un orden de clasificación descendente en los elementos de columna
`sortPriority`	• Número para indicar la prioridad de ordenación de la columna entre todas las columnas, cuanto más bajo sea el número, mayor será la prioridad • Sin valor, dejar en blanco para usar la prioridad de ordenación de columnas predeterminada • Valor `-1` para inhabilitar la prioridad de ordenación predeterminada de las columnas
`título`	Título de cabecera de columna, dejar en blanco para utilizar el título de cabecera predeterminado

Las columnas se muestran en el portlet en el mismo orden que el que se da en los objetos JSON que constituyen el valor del parámetro **columnas** . Sólo se muestran las columnas con identificadores de columna especificados en el valor, todas las demás están ocultas. Si se omite el valor del parámetro **columnas** , las columnas se muestran como están indicadas en el valor predeterminado mostrado en la primera fila de Tabla 42 en la página 152.

Los posibles valores para los identificadores de columna se describen en Tabla 44.

Tabla 44. Identificadores de columna válidos para el portlet Detalles

Identificador de columna	Descripción
`commonevents.id`	UUID dado para el suceso en tabla de sucesos comunes
`commonevents.externalEventid`	Identificador de suceso asignado por el remitente del suceso
`commonevents.specification`	Especificación de formato seguida del suceso, por ejemplo, `CAP`
`commonevents.eventType`	Valor no traducido para el código específico del sistema que indica si un suceso se ha escalado o no: `Suceso` o `Incidencia`
`commonevents.sent`	Hora enviada como la proporcionó el remitente del suceso

Tabla 44. Identificadores de columna válidos para el portlet Detalles (continuación)

Identificador de columna	Descripción
commonevents.headline	Texto de cabecera que describe el suceso
commonevents.hover text	Texto contextual que describe el suceso
commonevents.category	Valor de categoría no traducido
commonevents.certainty	valor de certeza no traducido
commonevents.severity	Valor de gravedad no traducido
commonevents.urgency	valor de urgencia no traducido
commonevents.url	dirección web de URL para obtener información adicional acerca del suceso
commonevents.externalWorkOrderId	Identificador de pedido de trabajo asociado, ID de Tivoli Service Request Manager procedimiento operativo estándar
commonevents.areaId	Identificador de área de mapa de asignación si el suceso está enlazado con un mapa de ubicación
commonevents.largeIcon	Icono utilizado para representar el suceso en el mapa
commonevents.largeHiliteIcon	Icono utilizado cuando el suceso se destaca en el mapa
commonevents.largeGreyIcon	Icono utilizado cuando el suceso se inhabilita en el mapa
commonevents.smallIcon	Icono utilizado para el suceso de la lista
commonevents.user1	El valor establecido en la política de Tivoli Netcool/Impact
commonevents.user2	Valor establecido por el usuario en la política de Tivoli Netcool/Impact
commonevents.user3	Valor establecido por el usuario en la política de Tivoli Netcool/Impact
commonevents.user4	Valor establecido por el usuario en la política de Tivoli Netcool/Impact
commonevents.user5	Valor establecido por el usuario en la política de Tivoli Netcool/Impact

Parámetro de condición

El valor del parámetro **condiciones** es una matriz de los objetos JSON que se pueden configurar como se describe en Tabla 45.

Tabla 45. Objetos en el valor de parámetro de condiciones del portlet Detalles

Tipo de objeto	Contiene
selector	Identificador de la columna a la que se aplica el operador

Tabla 45. Objetos en el valor de parámetro de condiciones del portlet Detalles (continuación)

Tipo de objeto	Contiene
`operator`	Operador de SQL que se aplica a los valores del selector; las opciones son: • `contains` cuando la columna de selector contiene el valor, esta opción es la predeterminada • `equals` cuando la columna de selector es igual al valor • `NotEquals` cuando la columna de selector no es igual al valor • `startsWith` cuando la columna de selector inicia con el valor • `endsWith` cuando la columna de selector termina con el valor
`values`	Valor de columna mostrado, el valor debe ser el valor de clave no traducido tal como se especifica en la tabla anterior

Nota:

El parámetro **`conditions`** define los criterios además de aquellos criterios proporcionados en el filtro del portlet de Mapa. Estos criterios sobrescriben las condiciones especificadas en el filtro de mapa o en la barra de herramientas.

Nota: La barra de herramientas está oculta por defecto.

Por ejemplo, necesita el siguiente cambio para las columnas:

- Muestre únicamente las columnas **Enviada**, **Titular**, **Categoría** y **URL** .
- Cambie el ancho de la columna **Enviada** a `12`.
- Cambie el formato de la columna **Enviada** a `d-MMM-yyyy HH:mm`.
- Cambie la prioridad de orden de clasificación de la columna **Enviado** a `2` y la columna **Categoría** a `1`.

Estos cambios se visualizan cuando entra lo siguiente en el campo **Columnas** y guarda las preferencias:

```
[{"id": "commonevents.sent", "width": "10", "format": "d-MMM-yyyy HH:mm", "sortPriority": "2"},
{"id": "commonevents.headline"},  {"id": "commonevents.category", "sortPriority": "1"}, {"id": "commonevents.url"}]
```

Por ejemplo, quiere mostrar únicamente sucesos que cumplen las siguientes condiciones:

- Una **Gravedad** de `Extremo` o `Grave`
- Un **Tipo de suceso** de `Incidencia`

Estos cambios se visualizan cuando entra la siguiente información en el campo **Condiciones** y guarda las preferencias:

```
[{"selector": "commonevents.severity", "operator": "equals", "values": ["Extreme", "Severe"]},
{"selector": "commonevents.eventType", "operator": "equals", "values": ["Incident"]}]
```

Conceptos relacionados:

"Detalles" en la página 278
Utilice el portlet Detalles para visualizar, supervisar y gestionar sucesos en IBM Intelligent Operations Center.

Valores del portlet Obtención de detalles de indicador clave de rendimiento

Personalice el portlet Obtención de detalles de indicador clave de rendimiento cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet Obtención de detalles de indicador clave de rendimiento . Los parámetros de personalización se describen en la siguiente tabla.

Tabla 46. Parámetros de personalización del portlet Obtención de detalles de indicador clave de rendimiento

Parámetro	Descripción	Valor predeterminado
Columnas	Especificaciones y orden de columnas que visualizar en la lista.	`[{"sortPriority":"1", "sortAscending":"true", "id":"kpi.NAME"}]`
Personalizar colores KPI	Colores utilizados en el portlet para indicar el estado de los KPI, por ejemplo, se puede escribir: `{"acceptable":"#7f7f7f", "take_action":"#34333"}` Los colores que entran aquí anulan los colores suministrados por la solución.	`{}`
JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`KpiDrillDownPortletHelp`
Habilitar filtro de KPI	Valor verdadero o falso para habilitar o inhabilitar un filtro de KPI de acuerdo con la información del valor de parámetro **`Filtro de KPI`**.	`false`
Ocultar barra de herramientas	Valor de verdadero o falso (true o false) para ocultar o visualizar la barra de herramientas en la parte superior del portlet.	`true`
KPI de filtro	ID de los indicadores clave de rendimiento que se mostrará cuando **`Habilitar filtro de KPI`** se establece `true` para el portlet, por ejemplo, puede escribir: `["Transportation","Airports", "Roads_and_Traffic", "Public_Safety","Fire_Department", "Water","Delayed_Flights", "Delayed_Flights_Airport_Two"]`	`[]`
Identificador de grupo del portlet	Nombre del grupo al que pertenece este portlet. Un nombre común configura la comunicación entre los portlets Obtención de detalles de indicador clave de rendimiento y Estado en la misma página.	`valor predeterminado`
Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`350`
Altura máxima del portlet	Número de píxeles que indica la altura máxima del portlet.	`600`
Título del portlet	Título para sustituir el título que se proporciona con la solución.	Si no se introduce un valor para este parámetro, el título suministrado por la solución que se muestra es el siguiente: Obtención de detalles de indicador clave de rendimiento.

Tabla 46. Parámetros de personalización del portlet Obtención de detalles de indicador clave de rendimiento (continuación)

Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica ningún paquete de recursos, no se busca ninguna clave y el título se muestra como proporcionado por la solución.	No hay paquete de recursos predeterminado.

Nota: La explicación de lo que ocurre con el título del portlet cuando se proporciona un paquete de recursos se aplica también al título de la columna que tiene su origen en el mismo paquete de recursos.

Parámetro Columnas

El valor del parámetro **Columnas** está en una matriz de objetos JSON que se puede configurar como se explica en la siguiente tabla.

Tabla 47. Objetos dentro del valor de parámetro Columnas del portlet Obtención de detalles de indicador clave de rendimiento

Objeto	Contiene
`sortPriority`	• Número para indicar la prioridad de ordenación de columna entre todas las columnas, cuanto más bajo sea el número, mayor será la prioridad • Sin valor, dejar en blanco para usar la prioridad de ordenación de columnas predeterminada • `-1` para inhabilitar la prioridad de ordenación de columnas predeterminada
`sortAscending`	• `true` para utilizar un orden de clasificación ascendente en los elementos de la columna • `false` para utilizar un orden de clasificación descendente en los elementos de la columna
`id`	identificador de columna para indicar que se va a mostrar la columna

Las columnas se muestran en el portlet en el mismo orden que el que se da en los objetos JSON que constituyen el valor del parámetro **columnas** . Sólo se muestran las columnas con identificadores de columna especificados en el valor, todas las demás están ocultas. Si se omite el valor del parámetro **columnas** , las columnas se muestran como están indicadas en el valor predeterminado mostrado en la primera fila de Tabla 46 en la página 157.

Los posibles valores para los identificadores de columna se describen en la siguiente tabla.

Tabla 48. Identificadores de columna válidos para el portlet Obtención de detalles de indicador clave de rendimiento

Identificador de columna	Descripción
`kpi.NAME`	Nombre del KPI
`kpi.CURRENT.VALUE`	Valor actual del KPI
`kpi.CURRENT.STATUS`	Estado actual del KPI
`kpi.CALCULATION.TIME`	Hora a la que se calculó el KPI

Conceptos relacionados:

"Obtención de detalles de indicador clave de rendimiento" en la página 281
Utilice el portlet Obtención de detalles de indicador clave de rendimiento para ver información adicional acerca de una categoría de ICR, el estado de sus ICR subyacentes.

Valores del portlet Indicadores clave de rendimiento

Personalice el portlet Indicadores clave de rendimiento cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet Indicadores clave de rendimiento . Los parámetros de personalización se describen en la siguiente tabla.

Tabla 49. Parámetros de personalización del portlet Indicadores clave de rendimiento

Parámetro	Descripción	Valor predeterminado
JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`KpiManagerPortletHelp`
Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`500`
Altura máxima del portlet	Número de píxeles que indica la altura máxima del portlet.	`600`
Título del portlet	Título para sustituir el título que se proporciona con la solución.	Si no se introduce un valor para este parámetro, el título suministrado por la solución que se muestra es el siguiente: Indicadores clave de rendimiento.
Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica ningún paquete de recursos, no se busca ninguna clave y el título se muestra como proporcionado por la solución.	No hay paquete de recursos predeterminado.

Conceptos relacionados:

"Indicadores clave de rendimiento" en la página 173
Utilice el portlet Indicadores clave de rendimiento para personalizar los indicadores clave de rendimiento (ICR) y su visualización jerárquica en IBM Intelligent Operations Center.

Valores del portlet Mapa de ubicación

Personalice el portlet Mapa de ubicación cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet. Los parámetros de personalización se describen en la siguiente tabla.

Tabla 50. Valores de parámetro de personalización del portlet Mapa de ubicación

Parámetro	Descripción	Valor predeterminado

Selecciones de filtro predeterminadas	Categorías de suceso predeterminadas que visualizar en el mapa. Escriba el nombre o los nombres separados por un punto y coma y sin espacios.	`CBRNE;Env;Fire;Geo;Health; Infra;Met;Rescue;Safety;Security; Transport;Other`
Color de resaltado de área predeterminado	Color predeterminado de una zona que se resalta cuando se pasa sobre el área con el cursor.	`#808080`
JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`LocationMapPortletHelp`
Selección de mapa predeterminado	Nombre del mapa de ubicación que se va a mostrar en el portlet.	`Miami SunLife Stadium`
Altura máxima del portlet	Número de píxeles que indica la altura máxima del portlet.	`600`
Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`400`
Identificador de grupo del portlet	Nombre del grupo al que pertenece este portlet. Un nombre común configura la comunicación entre los portlets Mapa, Detalles y Mapa de ubicación en la misma página.	`valor predeterminado`
Título del portlet	Título para sustituir el título que se proporciona con la solución.	Si no se introduce un valor para este parámetro, el título suministrado por la solución que se muestra es el siguiente: Mapa de ubicación.
Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica ningún paquete de recursos, no se busca ninguna clave y el título se muestra como proporcionado por la solución.	No hay paquete de recursos predeterminado.

Conceptos relacionados:

"Mapa de ubicación" en la página 282
Utilice el Mapa de ubicación portlet para ver los sucesos marcados en un mapa de ubicación. Un mapa de ubicación en IBM Intelligent Operations Center es un mapa o plano con zonas predefinidas para la interacción, por ejemplo, los asientos en un estadio deportivo.

Valores del portlet Gestor de mapas de ubicación

Personalice el portlet Gestor de mapas de ubicación cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet. Los parámetros de personalización se describen en la siguiente tabla.

Tabla 51. Valores de parámetro de personalización del portlet Gestor de mapas de ubicación

Parámetro	Descripción	Valor predeterminado
Color predeterminado de la nueva área seleccionada	Color predeterminado de un área del mapa determinada y seleccionada.	`#4AA02C`
Color predeterminado del área seleccionada guardada	Color predeterminado de un área del mapa guardada y seleccionada.	`#808080`
Color predeterminado de la nueva área	Color predeterminado de un área del mapa determinada.	`#009900`
Color predeterminado del área guardada	Color predeterminado de un área del mapa guardada.	`#808080`
JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`LocationMapManagerPortletHelp`
Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`400`
Título del portlet	Título para sustituir el título que se proporciona con la solución.	Si no se introduce un valor para este parámetro, el título suministrado por la solución que se muestra es el siguiente: Gestor de mapas de ubicación.
Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica ningún paquete de recursos, no se busca ninguna clave y el título se muestra como proporcionado por la solución.	No hay paquete de recursos predeterminado.

Conceptos relacionados:

"Gestor de mapas de ubicación" en la página 181
Utilice el portlet Gestor de mapas de ubicación para personalizar el portletMapa de ubicación .

Valores del portlet Mapa

Personalice el portlet Mapa cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet Mapa . Los parámetros de personalización se describen en la siguiente tabla.

Tabla 52. Valores de los parámetros de personalización

Parámetro	Descripción	Valor predeterminado

Tabla 52. Valores de los parámetros de personalización (continuación)

Latitud central	Coordenadas específicas para establecer el punto central del mapa. La ubicación actual del mapa se muestra a la derecha de los campos. Puede acercarse o enfocar al mapa hacia su ubicación deseada, a continuación, cortar y pegar los valores mostrados en los campos correspondientes.	25.780416
Longitud central		-80.203629
Nivel de zoom	Nivel de ampliación estándar para el mapa. El rango de los niveles de zoom válidos disponibles depende del mapa base. En general, el intervalo es de 1 en adelante. El valor de 1 es el nivel más bajo de zoom que muestra el mapa en su aumento más bajo. Por ejemplo, el mapa base ArcGIS predeterminado suministrado con la solución muestra el detalle geográfico hasta un nivel de zoom máximo de 12.	11
Tipo de capa base	Valor para el tipo de mapa base	ARC_GIS_REST
URL de capa base	URL del mapa base. La URL debe contener, en el orden correcto, los marcadores de posición que representan las coordenadas x, y y z del mapa. Puede seleccionar un mapa desde el servidor Esri GIS instalado o desde un servicio GIS públicamente disponible.	http://services.arcgisonline.com/ArcGIS/rest/services/World_Street_Map/MapServer/tile/${z}/${y}/${x}
Fuente KML o URL de archivo	URL para mostrar los datos KML. Entre una URL para una ubicación en el mismo servidor que el portlet con el mismo dominio y puerto. Para garantizar que implementa esta condición, entre únicamente URL que comiencen con'/' o el carácter de barra inclinada, así el navegador selecciona el dominio y puerto actual. Para múltiples cadenas de URL utilice un punto y coma y que sin espacios entre las URL. Si el sitio web no es local, utilice un servidor proxy en su servidor local para acceder al sitio. **Nota:** Utilice esta opción para pequeños ajustes locales, pero tenga en cuenta la cantidad de datos implicados para que no se sobrecargue la visualización o afecte al rendimiento.	No se ha proporcionado ningún valor predeterminado con la solución.

Tabla 52. Valores de los parámetros de personalización (continuación)

Cantidad de elementos a mostrar	Límite para el número de marcadores mostrados en una vista. Entre el número máximo de marcadores que se pueden mostrar. Si el número de marcadores del área del mapa en la vista supera este límite, no se muestran los marcadores y aparece un mensaje de aviso. El usuario puede elegir si carga los marcadores o cambia la vista.	`250`
Selecciones de filtro predeterminadas	Categorías de suceso predeterminadas que visualizar en el mapa. Escriba el nombre o los nombres separados por un punto y coma y sin espacios.	`CBRNE;Env;Fire;Geo; Health;Infra;Met;Rescue; Safety;Security;Transport; Otros`
Altura máxima del portlet	Número de píxeles que indica la altura máxima del portlet.	`600`
Identificador de grupo del portlet	Nombre del grupo al que pertenece este portlet. Un nombre común configura la comunicación entre los portlets Mapa, Detalles y Mapa de ubicación en la misma página.	`valor predeterminado`
Título del portlet	Título para sustituir el título que se proporciona con la solución.	Si no se introduce un valor para este parámetro, el título suministrado por la solución que se muestra es el siguiente: Mapa.
JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`NavigatorPortletHelp`
Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica ningún paquete de recursos, no se busca ninguna clave y el título se muestra como proporcionado por la solución.	No hay paquete de recursos predeterminado.

Conceptos relacionados:

"Mapa" en la página 285
Uso del portlet Mapa para ver sucesos y recursos en un mapa.

Valores del portlet Mis actividades

Personalice el portlet Mis actividades cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet Mis actividades . Los parámetros de personalización se describen en la siguiente tabla.

Tabla 53. Parámetros de personalización del portlet Mis actividades

Parámetro	Descripción	Valor predeterminado
JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`ActivitiesPortletHelp`
Identificador de grupo del portlet	Nombre del grupo al que pertenece este portlet. Un nombre común configura la comunicación entre los portlets en la misma página. Por ejemplo, un nombre común puede establecer la comunicación entre los portlets Mis actividades y Detalles.	`valor predeterminado`
Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`200`
Altura máxima del portlet	Número de píxeles que indica la altura máxima del portlet.	`600`
Título del portlet	Título para sustituir el título que se proporciona con la solución.	Si no se introduce un valor para este parámetro, el título suministrado por la solución que se muestra es el siguiente: Mis actividades.
Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica ningún paquete de recursos, no se busca ninguna clave y el título se muestra como proporcionado por la solución.	No hay paquete de recursos predeterminado.

Conceptos relacionados:

"Mis actividades" en la página 290
El portlet Mis actividades muestra una lista dinámica de actividades que son propiedad del grupo del que es miembro el usuario que tiene sesión iniciada en la interfaz.

Valores del portlet Notificaciones

Personalice el portlet Notificaciones cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet Notificaciones . Los parámetros de personalización se describen en la siguiente tabla.

Tabla 54. Parámetros de personalización del portlet Notificaciones

Parámetro	Descripción	Valor predeterminado
Columnas	Especificaciones y orden de columnas que visualizar en la lista.	`[{"id": "notifications.HEADLINE"},{"id": "notifications.SENTFROM"},{"id": "notifications.SENTTIME", "width" : "10", "format": "yyyy-MM-dd HH:mm:ss"}]`

Tabla 54. Parámetros de personalización del portlet Notificaciones (continuación)

JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`CityCoordinatorPortletHelp`
Ocultar barra de herramientas	Valor de verdadero o falso (true o false) para ocultar o visualizar la barra de herramientas en la parte superior del portlet.	`true`
Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`200`
Altura máxima del portlet	Número de píxeles que indica la altura máxima del portlet.	`600`
Título del portlet	Título para sustituir el título que se proporciona con la solución.	Si no se introduce un valor para este parámetro, el título suministrado por la solución que se muestra es el siguiente: Notificaciones.
Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica ningún paquete de recursos, no se busca ninguna clave y el título se muestra como proporcionado por la solución.	No hay paquete de recursos predeterminado.

Nota: La explicación de lo que ocurre con el título del portlet cuando se proporciona un paquete de recursos se aplica también al título de la columna que tiene su origen en el mismo paquete de recursos.

Parámetro Columnas

El valor del parámetro **`Columnas`** está en una matriz de objetos JSON que se puede configurar como se explica en Tabla 55.

Tabla 55. Objetos dentro del valor de parámetro Columnas del portlet Notificaciones

Objeto	**Contiene**
`id`	identificador de columna para indicar que se va a mostrar la columna
`width`	Número de píxeles que indica el ancho de columna
`formato`	Cadena que representa el formato que se utilizará para las columnas de fecha y hora, la entrada sobrescribe el valor de la tabla `sysprop`
`sortAscending`	• `true` para utilizar un orden de clasificación ascendente en los elementos de la columna • `false` para utilizar un orden de clasificación descendente en los elementos de la columna

Tabla 55. Objetos dentro del valor de parámetro Columnas del portlet Notificaciones (continuación)

Objeto	Contiene
`sortPriority`	• Número para indicar la prioridad de ordenación de la columna entre todas las columnas, cuanto más bajo sea el número, mayor será la prioridad • Sin valor, dejar en blanco para usar la prioridad de ordenación de columnas predeterminada • `-1` para inhabilitar la prioridad de clasificación de columnas predeterminada
`título`	Título de cabecera de columna, dejar en blanco para utilizar el título de cabecera predeterminado

Las columnas se muestran en el portlet en el mismo orden que el que se da en los objetos JSON que constituyen el valor del parámetro **`columnas`** . Sólo se muestran las columnas con identificadores de columna especificados en el valor, todas las demás están ocultas. Si se omite el valor del parámetro **`columnas`** , las columnas se muestran como están indicadas en el valor predeterminado mostrado en la primera fila de Tabla 54 en la página 164.

Los posibles valores para los identificadores de columna se describen en Tabla 56.

Tabla 56. Identificadores de columna válidos para el portlet Notificaciones

Identificador de columna	Descripción
`notifications.ID`	UUID dado para la notificación en la tabla de notificaciones
`notifications.CATEGORY`	Valor no traducido de la categoría del suceso o del KPI relacionado con la notificación
`notifications.SENTFROM`	Servicio que ha generado la notificación
`notifications.SENTTOGROUP`	Lista de grupos que pueden acceder a la notificación
`notifications.SENTTIME`	Hora generada por el servicio que ha enviado la notificación
`notifications.HEADLINE`	Texto breve que describe la notificación
`notifications.DESCRIPTION`	Texto detallado que describe la notificación
`notifications.ALERTLINK`	Lista de alertas CAP relacionadas con la notificación
`notifications.KPILINK`	KPI relacionado con la notificación

Conceptos relacionados:

"Notificaciones" en la página 293
Utilice el portlet Notificaciones para ver sus mensajes de alerta y sus detalles.

Valores del portlet Informes

Personalice el portlet Informes cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet. Los parámetros de personalización se describen en la siguiente tabla.

Tabla 57. Valores de parámetro de personalización del portlet Informes

Parámetro	Descripción	Valor predeterminado

Tabla 57. Valores de parámetro de personalización del portlet Informes (continuación)

JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`ReportsIntegrationPortletHelp`
Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`600`
Altura máxima del portlet	Número de píxeles que indica la altura máxima del portlet.	`800`
Título del portlet	Título del portlet Informes .	`Informe personalizado`
URL de informe	Especifica el URL del informe que se visualiza.	`http://ioc1bvtlite1.rtp.raleigh.ibm.com/cognos/ServletGateway/servlet/Gateway?b_action=cognosViewer&ui.action=run&ui.object=%2fcontent%2fpackage%5b%40name%3d%27ioc_cap_model%27%5d%2ffolder%5b%40name%3d%27reports%27%5d%2ffolder%5b%40name%3d%27User_defined_reports%27%5d%2freport%5b%40name%3d%27User_defined_report%27%5d&ui.name=User_defined_report&run.outputFormat=&run.prompt=true&cv.toolbar=false&cv.header=false`
Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica el paquete de recursos, no se busca la clave y el título se muestra como se muestra en el campo Título del portlet de la ventana **Valores compartidos**.	No hay paquete de recursos predeterminado.
Mostrar campo de URL en la página	Seleccione **True** para incluir el botón **URL de informe** en la página del portlet Informes. Este botón permite a todos los usuarios, no sólo a los administradores, crear un informe personalizado y definir el URL de informe. Seleccione **False** (falso) para omitir el botón **URL de informe** de la página del portlet Informes.	`False`

Conceptos relacionados:

"Informes " en la página 294
Utilice el portlet Informes para ver un informe de sucesos como gráfico. El portlet proporciona varias opciones para agrupar suceso y puede elegir sucesos por un rango de fechas o por una fecha concreta. Estos informes le ayudan a planificar respuestas para sucesos actuales o futuros.

Valores del portlet Ejemplo de aplicación de publicación

Personalice el portlet Ejemplo de aplicación de publicación cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet Ejemplo de aplicación de publicación . Los parámetros de personalización se describen en la siguiente tabla.

Tabla 58. Parámetros de personalización del portlet Ejemplo de aplicación de publicación

Parámetro	Descripción	Valor predeterminado
JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`SamplePublisherPortletHelp`
Título del portlet	Título para sustituir el título que se proporciona con la solución.	Si no se introduce un valor para este parámetro, el título suministrado por la solución que se muestra es el siguiente: Ejemplo de aplicación de publicación.
Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica ningún paquete de recursos, no se busca ninguna clave y el título se muestra como proporcionado por la solución.	No hay paquete de recursos predeterminado.

Conceptos relacionados:

"Ejemplo de aplicación de publicación" en la página 107
Utilice el portlet Ejemplo de aplicación de publicación para publicar sucesos de Common Alerting Protocol (CAP) en IBM Intelligent Operations Center.

Valores del portlet Procedimientos operativos estándar

Personalice el portlet Procedimientos operativos estándar cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet Procedimientos operativos estándar . Los parámetros de personalización se describen en la siguiente tabla.

Tabla 59. Parámetros de personalización del portlet Procedimientos operativos estándar

Parámetro	Descripción	Valor predeterminado
JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`SOPManagerPortletHelp`
Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`440`

Conceptos relacionados:

"Procedimientos operativos estándar" en la página 131
Puede definir procedimientos de operación estándar y actividades para gestionar sucesos que vienen con IBM Intelligent Operations Center. Utilice el portlet Procedimientos operativos estándar para acceder a las aplicaciones procedimiento operativo estándar, matriz de selección del procedimiento de operación estándar y diseñador del flujo de trabajo en Tivoli Service Request Manager.

Valores del portlet Estado

Personalice el portlet Estado cambiando los valores en los campos de la ventana **Valores compartidos** .

Parámetros de personalización

Los campos de la ventana **Valores compartidos** contiene los valores de los parámetros de personalización para el portlet Estado . Los parámetros de personalización se describen en la siguiente tabla.

Tabla 60. Parámetros de personalización del portlet Estado

Parámetro	Descripción	Valor predeterminado
Personalizar colores KPI	Colores utilizados en el portlet para indicar el estado de los KPI, por ejemplo, se puede escribir: `{"acceptable":"#7f7f7f", "take_action":"#34333"}` Los colores que entran aquí anulan los colores suministrados por la solución.	{}
JSP de ayuda predeterminadas	Nombre del archivo de ayuda JSP que mostrar cuando se selecciona la ayuda desde el menú del portlet.	`KpiStatusPortletHelp`
Habilitar filtro de KPI	Valor verdadero o falso para habilitar o inhabilitar un filtro de KPI adicional para el portlet de acuerdo con la información del valor de parámetro **`Filtro de KPI`**.	`false`
KPI de filtro	ID de KPI que se mostrarán cuando se establezca 'Habilitar filtro de KPI' en verdadero para el portlet, por ejemplo: `["Transportation","Airports", "Roads_and_Traffic","Public_Safety", "Fire_Department", "Water","Delayed_Flights", "Delayed_Flights_Airport_Two"]`	[]
Identificador de grupo del portlet	Nombre del grupo al que pertenece este portlet. Un nombre común configura la comunicación entre los portlets Obtención de detalles de indicador clave de rendimiento y Estado en la misma página.	`valor predeterminado`
Altura del portlet	Número de píxeles que indica la altura estándar del portlet.	`200`
Altura máxima del portlet	Número de píxeles que indica la altura máxima del portlet.	`600`
Título del portlet	Título para sustituir el título que se proporciona con la solución.	Si no se introduce un valor para este parámetro, el título suministrado por la solución que se muestra es el siguiente: Estado.

Tabla 60. Parámetros de personalización del portlet Estado (continuación)

Paquete de recursos	Ubicación del paquete de recursos proporcionado como origen del valor de las propiedades; por ejemplo, el título de portlet. Esta ubicación es obligatoria si desea especificar el título como una clave de propiedad en un paquete de recursos que proporcione. Si no se especifica ningún paquete de recursos, no se busca ninguna clave y el título se muestra como proporcionado por la solución.	No hay paquete de recursos predeterminado.
Mostrar leyenda	Valor de verdadero o falso (true o false) para ocultar o visualizar la leyenda en el portlet.	`true`
Orden	Propiedad KPI por la que se ordena la lista de KPI. El valor predeterminado es ordenar en orden alfabético ascendente por nombre de KPI. Otras opciones son `kpi.CURRENT.VALUE`, `kpi.CURRENT.STATUS` y `kpi.CALCULATION.TIME`	`+kpi.NAME`

Conceptos relacionados:

"Estado" en la página 297
Utilice el portlet Estado para ver el estado de los indicadores clave de rendimiento (ICR) para una única organización o en varias organizaciones.

Personalización de la ayuda de portlet

Puede desplegar una ayuda alternativa para un portlet de IBM Intelligent Operations Center.

Acerca de esta tarea

Para obtener ayuda sobre el uso de cada portlet, haga clic en la esquina superior derecha del portlet y seleccione **Ayuda** en el menú que aparece.

Si cambia el diseño o los datos mostrados en un portlet, es posible que desee cambiar también la ayuda mostrada.

Procedimiento

1. Cree la ayuda alternativa como un archivo JSP.
2. Puede denominar el archivo como prefiera, pero debe usar el sufijo correcto de su idioma. La configuración de idioma se basa en el idioma del navegador. Utilice el identificador del entorno local estándar del idioma que corresponda, por ejemplo:

Opción	Descripción
_pt_BR	Portugués (Brasil)
_en	Inglés
_fr	Francés
_de	Alemán
_es	Español

3. Utilice la ventana **Configuración compartida** para establecer el parámetro **`DefaultHelpJSP`** con el nombre del archivo de ayuda alternativo. No incluya el sufijo de idioma ni la extensión de archivo .jsp.
4. Copie el archivo JSP de ayuda alternativo a la ubicación correcta: `/opt/IBM/WebSphere/wp_profile/installedApps/cell1/ioc_portal_ear.ear/`*`war_portlet`*`/`*`raíz_portlet`*`/jsp/html/help`. Los valores de los portlets de las variables *war_portlet* y *raíz_portlet* se listan en un tema separado. Consulte el enlace que encontrará al final de este tema para obtener una lista de estos valores.

Nota: Al cambiar el archivo de ayuda de Resumen de permisos de usuario, sustituya `ioc_portal_ear.ear` con `iss_portal_ear.ear` en la vía de acceso proporcionada en este paso.

Qué hacer a continuación

Proporcione traducciones del archivo de ayuda alternativo para todos los idiomas soportados, incluido un idioma predeterminado.

Información relacionada:

Documentación del producto IBM WebSphere Portal 7

Ubicaciones de archivo de ayuda de portlet

Los valores de ubicación son necesarios para los portlets cuando se sustituye la ayuda del portlet predeterminado con el archivo de ayuda JSP alternativo.

La Tabla 1 y 2 proporcionan valores para la ubicación de los archivos de ayuda del portlet del usuario y de administración.

Tabla 61. Valores de portlet de usuario para la ubicación de un archivo de ayuda alternativo

Portlet	*portlet_war*	*portlet_root*
Detalles	icoc_ui_common_events_portlet.war	_icoc_ui_common_events_portlet
Obtención de detalles de indicador clave de rendimiento	icoc_ui_kpi_drilldown_portlet.war	_icoc_ui_kpi_drilldown_portlet
Mapa de ubicación	icoc_ui_location_map_portlet.war	_icoc_ui_location_map_portlet
Mapa	icoc_ui_navigator_portlet.war	_icoc_ui_navigator_portlet
Mis actividades	icoc_ui_activities_portlet.war	_icoc_ui_activities_portlet
Notificaciones	icoc_ui_city_coordinator_portlet.war	_icoc_ui_city_coordinator_portlet
Informes	icoc_ui_reports_portlet.war	_icoc_ui_reports_portlet
Estado	icoc_ui_kpi_status_portlet.war	_icoc_ui_kpi_status_portlet

Tabla 62. Valores de portlet de administración para la ubicación de un archivo de ayuda alternativo

Portlet	*portlet_war*	*portlet_root*
Consolas de administración	icoc_ui_administration_console_portlet.war	_icoc_ui_administration_console_portlet
Script de suceso	icoc_ui_event_scripting_portlet.war	_icoc_ui_event_scripting_portlet
Indicadores clave de rendimiento	icoc_ui_kpi_manager_portlet.war	_icoc_ui_kpi_manager_portlet
Gestor de mapas de ubicación	icoc_ui_location_map_manager_portlet.war	_icoc_ui_location_map_manager_portlet
Ejemplo de aplicación de publicación	icoc_ui_sample_publisher_portlet.war	_icoc_ui_sample_publisher_portlet
Procedimientos operativos estándar	icoc_ui_sop_manager_portlet.war	_icoc_ui_sop_manager_portlet
Resumen de permisos de usuario	iss_ui_security_portlet.war	_iss_ui_security_portlet

Personalización de los ICR

En IBM Intelligent Operations Center, puede personalizar los modelos de indicador clave de rendimiento (KPI) para que se adapten a sus procesos empresariales.

Los KPI están diseñados para proporcionar datos estadísticos que se pueden utilizar para analizar tendencias o indicar áreas problemáticas. Los datos KPI se actualizan por medio de sucesos de IBM Intelligent Operations Center.

El IBM Intelligent Operations Center proporciona un conjunto de sucesos y KPI de muestra que se pueden utilizar para actualizar el estado del KPI. Hay tres modelos de KPI de muestra proporcionados con IBM Intelligent Operations Center que se basan en seguridad pública de muestra, transporte y supervisión de agua y procesos empresariales. Para obtener más información acerca de los KPI de muestra proporcionados con IBM Intelligent Operations Center, siga el enlace al final del tema.

Cada solución de IBM Intelligent Operations Center sigue una creación de KPI y un proceso de integración para configurar los KPI necesarios para el entorno empresarial específico. Puede crear sus propios modelos de KPI con IBM WebSphere Business Monitor. Para obtener más información sobre la creación e integración de KPI con IBM Intelligent Operations Center, siga el enlace al final del tema.

Utilice el portlet Indicadores clave de rendimiento para personalizar los ICR en IBM Intelligent Operations Center. El portlet Indicadores clave de rendimiento se proporciona para el administrador como una de las opciones de las **Herramientas de personalización de la solución** .

Utilizando el portlet, puede ver las propiedades de KPI; crear, copiar o modificar KPI; y ver o cambiar las visualizaciones jerárquicas para modelos KPI.

Utilice la pestaña **Definición de KPI** para definir los KPI asociados con un modelo KPI específico en IBM Intelligent Operations Center:

- Visualice la lista actual d KPI que pertenece a un modelo de KPI.
- Visualice las propiedades de un KPI existente.
- Actualice las propiedades de un KPI existente.
- Cree un nuevo KPI para un modelo de KPI:
  - Agregue KIP calculados utilizando una métrica definida
  - Valor KPI de expresión basado en otros KPI
- Suprima un KPI.

Las actualizaciones se guardan en modelos de IBM WebSphere Business Monitor almacenados en la base de datos de IBM Intelligent Operations Center . Las actualizaciones también se reflejan en la próxima renovación de los portletsEstado y Obtención de detalles de indicador clave de rendimiento .

Utilice la pestaña **Jerarquía de visualización de KPI** para actualizar las jerarquías de KPI visualizadas en los portlets Estado y Obtención de detalles de indicador clave de rendimiento .

- Visualice las jerarquías KPI existentes.
- Visualice las propiedades principales de un KPI.
- Cambie la estructura de árbol moviendo o eliminando elementos en una jerarquía de KPI.
- Añada KPI predefinidos a una jerarquía.

Las actualizaciones se reflejan en la próxima renovación de los portletsEstado y Obtención de detalles de indicador clave de rendimiento .

Nota: Las actualizaciones para la jerarquía de visualización son independientes del modelo de KPI y se necesita comprender el modelo de KPI para garantizar que las actualizaciones se adhieran a la lógica del modelo de KPI.

Conceptos relacionados:

"Creación e integración de KPI" en la página 113
Los modelos de KPI se pueden crear y modificar utilizando un kit de herramientas de desarrollo de supervisión de negocio y un portlet de gestión de KPI.

"KPI de muestra" en la página 125
Los KPI de muestra se proporcionan con IBM Intelligent Operations Center. Los KPI de muestra están diseñados para facilitar la implementación de distintos tipos de KPI utilizando IBM WebSphere Business Monitor Development Toolkit. Se proporcionan modelos de supervisión de muestra para agua, transporte y seguridad pública.

Indicadores clave de rendimiento

Utilice el portlet Indicadores clave de rendimiento para personalizar los indicadores clave de rendimiento (ICR) y su visualización jerárquica en IBM Intelligent Operations Center.

En el portlet Indicadores clave de rendimiento puede ver, cambiar, copiar, crear y suprimir KPI. También puede personalizar las jerarquías de ICR que aparecen en los portlets Estado y Obtención de detalles de indicador clave de rendimiento.

Para acceder al portlet Indicadores clave de rendimiento, en la interfaz de administración de WebSphere Portal haga clic en **Intelligent Operations** > **Herramientas de personalización** > **Indicadores clave de rendimiento**.

Visualización de las jerarquías de KPI

Utilice la pestaña **Relaciones y visualización** para ver los modelos de KPI cuando se despliegan en los portlets Estado y Obtención de detalles de indicador clave de rendimiento .

Acerca de esta tarea

En la parte izquierda de la ventana **Relaciones y visualización** , ve enumerados los nodos de nivel raíz para las jerarquías de KPI que está autorizado a ver. Estos nodos representan los modelos de KPI como se muestran en los portlets Estado y Obtención de detalles de indicador clave de rendimiento .

Procedimiento

1. Expanda el nodo de nivel raíz para ver los niveles inferiores del árbol de modelos que desea ver.
2. Pulse el título del nodo de nivel raíz para previsualizar los detalles en la parte derecha de la ventana. La información se muestra como se describe en la siguiente tabla:

Opción	Descripción
Nombre	El título del nodo de nivel raíz.
Tipo	El tipo del nodo de nivel raíz.
ID del modelo	identificador para el correspondiente modelo de KPI
Categoría	clasificación del modelo
Icono	icono que representa el nodo de nivel raíz

3. Haga clic en un ICR para obtener una previsualización de sus detalles a la derecha de la ventana **Relaciones y visualización**.

Cambio de una jerarquía de ICR

Utilice la pestaña **Relaciones y visualización** para cambiar o eliminar un modelo de KPI cuando se visualiza en los portlets Estado y Obtención de detalles de indicador clave de rendimiento .

Procedimiento

1. En la parte derecha de la ventana **Relaciones y visualización** , pulse el nodo de nivel raíz y los subelementos para expandir el árbol jerárquico al nivel que desea.
2. Puede mover, añadir, cambiar o eliminar elementos existentes, de la siguiente forma:
   - Para mover subelementos dentro de un árbol, arrastre el elemento a la posición deseada. Los indicadores verde o rojo indican si una acción está permitida o no.
   - Para agregar a un árbol desde la lista de subelementos existentes para un modelo de ICR, haga clic en el elemento que contendrá el subelemento y haga clic en **Agregar ICR**.
   - Para ir a la ventana **Propiedades de KPI** y cambiar un subelemento, pulse con el botón derecho del ratón sobre el elemento y pulse **Editar**.
   - Para eliminar un nodo de nivel raíz o un subelemento de un árbol, haga clic con el botón derecho del ratón en dicho elemento y haga clic en **Eliminar**. Eliminando un elemento de nodo raíz, elimina todos los subelementos que contiene.
3. Haga clic en **Guardar** para guardar las actualizaciones.

   Nota: Aquí no es posible editar el nombre de una organización propietaria o nodo de nivel raíz. Si desea cambiar una organización propietaria, elimínela y sustitúyala con otro nombre.

Añadir una organización propietaria

Utilice la pestaña **Relaciones y visualización** para añadir el nodo de nivel raíz que se va a visualizar en los portlets Estado y Obtención de detalles de indicador clave de rendimiento .

Procedimiento

1. En la parte superior izquierda de la ventana **Relaciones y visualización**, haga clic en **Añadir organización propietaria**.
2. Escriba un nombre de visualización.
3. En la lista desplegable del campo **Modelo** , seleccione el nodo de nivel raíz que se va a añadir.
4. En la lista desplegable del campo **Categoría** seleccione una categoría para el nodo de nivel raíz.
5. En la lista desplegable del campo **Icono** , seleccione el nombre de archivo para el icono que va a representar el nodo de nivel raíz.
6. Pulse **Aceptar** para añadir el nuevo nodo en la parte izquierda de la ventana **Relaciones y visualización** .
7. Haga clic en **Guardar** para actualizar la visualización en los portlets Estado y Obtención de detalles de indicador clave de rendimiento.

Cambio de la leyenda de ICR

Utilice la pestaña **Relaciones y visualización** para cambiar la leyenda de KPI en el portletEstado .

Procedimiento

1. En la parte superior izquierda de la ventana **Relaciones y visualización**, haga clic en **Leyenda de ICR**.
2. Cambie la visualización para la leyenda de ICR del siguiente modo:
   - Para añadir un rango, pulse **Añadir fila**.
   - Para cambiar un rango, edite los campos en **Nombre de rango**, **Color**, **Icono**.
   - Para eliminar un rango, haga clic en **Eliminar**.
3. Haga clic en **Aceptar** para actualizar la visualización en los portlets Estado y Obtención de detalles de indicador clave de rendimiento.

Visualización de un modelo de ICR

Utilice la pestaña **Definición de ICR** para ver los ICR que pertenecen a los modelos de ICR que hay en IBM Intelligent Operations Center.

Procedimiento

El campo **Filtrar por modelo** contiene una lista desplegable de los modelos de proceso de negocio que está autorizado a ver. Seleccione todos los modelos o el modelo para el que desea ver los KPI. La información de KPI se muestra tal y como se describe en la siguiente tabla:

Opción	Descripción
Nombre de ICR	El título del ICR. Puede hacer clic en el nombre de ICR para ver las propiedades.
Modelo	El nombre del modelo al que pertenece el ICR.
Creado	Método de creación del KPI: • Un KPI modelado es un KPI creado a nivel de modelo utilizando IBM WebSphere Business Monitor. • Un KPI de panel de control es un KPI creado utilizando un portletIndicadores clave de rendimiento .
Tipo	Tipo de KPI: • Un KPI agregado tiene un valor basado en el método de medición y de agregación que seleccione. • Un KPI de expresión tiene un valor que se basa en otros KPI o funciones definidas por el usuario, utilizando la expresión XPath que define.
Acceso	Nivel de acceso de un ICR: • Un KPI compartido es un KPI que pueden ver otros usuarios que tienen acceso. • Un KPI privado es un KPI que no se puede compartir con otros usuarios que no sea el propietario.

Visualización o cambio de un KPI

Utilice la pestaña **Definición de ICR** para ver o cambiar un ICR existente que pertenezca a un modelo de IBM Intelligent Operations Center.

Procedimiento

1. Seleccione un ICR. En la parte superior izquierda de la ventana **Definición de ICR**, haga clic en **Editar**. Se abre la ventana **Propiedades de ICR**.
2. Para cambiar el ICR, edite los campos en las pestañas de la ventana de propiedades. Para obtener más detalles acerca de la edición de estos campos para crear un KPI de expresión o un KPI agregado, pulse el enlace al final del tema.

   Nota: No puede cambiar la definición de un KPI modelado aquí.
3. Para guardar y salir de la ventana de **Propiedades de KPI** actualizada, pulse **Aceptar**. Para guardar y seguir cambiando el ICR copiado, haga clic en **Aplicar**. Para salir sin guardar, haga clic en **Cancelar**.

Copia de un KPI

Utilice la pestaña **Definición de KPI** para hacer una copia de un KPI existente para un modelo enIBM Intelligent Operations Center.

Procedimiento

1. Seleccione un ICR. En la parte superior izquierda de la ventana **Definición de ICR**, haga clic en **Más acciones** > **Copiar**. Se abre la ventana **Propiedades de ICR**.
2. Escriba un nuevo nombre de ICR en el campo **Nombre de ICR**.
3. Edite las propiedades del KPI copiado según los pasos 3 y 4 de procedimiento para cambiar un KPI.

Creación de un KPI

Utilice la pestaña **Definición de KPI** para crear un KPI para un modelo en IBM Intelligent Operations Center.

Procedimiento

1. En la parte superior izquierda de la ventana **Definición de ICR**, haga clic en **Crear**.
2. Haga clic en **Nuevo ICR agregado** o en **Nuevo ICR de expresión**. Se abre la ventana **Propiedades de ICR**.
3. Edite las propiedades del nuevo KPI según los pasos 3 y 4 de procedimiento para cambiar un KPI.

Qué hacer a continuación

Para obtener más información sobre la creación de KPI, siga el enlace de la documentación de IBM Websphere Business Monitor que encontrará al final de este tema.

KPI de muestra

Con la solución se proporciona un conjunto de ICR de muestra. Estos ICR se han diseñado para brindar orientación para planificación e implementación de distintos tipos de ICR que se adecuen a su organización. Se proporcionan ejemplos para las áreas de agua, transporte y seguridad pública.

Personalización del portlet Indicadores clave de rendimiento

Puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Conceptos relacionados:

"Estado" en la página 297
Utilice el portlet Estado para ver el estado de los indicadores clave de rendimiento (ICR) para una única organización o en varias organizaciones.

"Obtención de detalles de indicador clave de rendimiento" en la página 281
Utilice el portlet Obtención de detalles de indicador clave de rendimiento para ver información adicional acerca de una categoría de ICR, el estado de sus ICR subyacentes.

Referencia relacionada:

"Valores del portlet Indicadores clave de rendimiento" en la página 159
Personalice el portlet Indicadores clave de rendimiento cambiando los valores en los campos de la ventana **Valores compartidos** .

Información relacionada:

 Centro de información de IBM WebSphere Business Process Management Versión 7.0

Copia de seguridad antes de personalizar KPI

Realice copias de seguridad y restaure los KPI creados o modificados con IBM WebSphere Business Monitor o con el portlet de Indicadores clave de rendimiento.

Acerca de esta tarea

Antes de personalizar los modelos de KPI y modificar los KPI, se recomienda que realice una copia de seguridad de los modelos existentes. El procedimiento de este tema exporta todos los KPI del modelo especificado al archivo especificado e importa los KPI del archivo especificado al modelo especificado.

Procedimiento

1. Inicie sesión en servidor de aplicaciones.
2. Cambie al directorio `bin` del perfil de IBM WebSphere Business Monitor: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin`

3. Para exportar los KPI, ejecute el mandato: `./wsadmin.sh -wsadmin_classpath "../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../scripts.wbm/kpi/exportKpis.jy" "`*`vía_acceso_archivo_xml`*`" `*`ID_modelo versión_modelo`* `TODO`

   vía_acceso_archivo_xml es el nombre y la vía de acceso del archivo XML al cual está exportando los KPI. *ID_modelo* y *versión_modelo* son el ID y la versión del modelo de KPI desde donde está exportando los KPI.
4. Para importar los KPI, ejecute el mandato: `./wsadmin.sh -wsadmin_classpath "../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../scripts.wbm/kpi/importKpis.jy" "`*`vía_acceso_archivo_xml`*`"`

   vía_acceso_archivo_xml es el nombre y la vía de acceso del archivo XML desde donde está importando los KPI.

Ejemplo

Para exportar todos los KPI del modelo `icoc_sample_public_safety_monitor_model` a `/tmp/kpis.xml`, ejecute el mandato siguiente. En el mandato, el valor de *vía_acceso_archivo_xml* es `/tmp/kpis.xml`, el valor de *ID_modelo* es `icoc_sample_public_safety_monitor_model` y el valor de *versión_modelo* es `2011-02-18T10:49:46`.

```
./wsadmin.sh -wsadmin_classpath "../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:
../../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../scripts.wbm
/kpi/exportKpis.jy" "/tmp/kpis.xml" icoc_sample_public_safety_monitor_model
2011-02-18T10:49:46 ALL
```

Para obtener más información, consulte el enlace al centro de información de WebSphere Business Monitor al final de este tema.

Referencia relacionada:

"Copia de seguridad de datos" en la página 265
Para evitar la pérdida de datos valioso en IBM Intelligent Operations Center, realice una copia de seguridad de determinados archivos, directorios y bases de datos a intervalos regulares.

Información relacionada:

IBM Smarter Cities Software Solutions Redbooks

Personalización de la correlación de sucesos

En esta sección se explica la correlación de sucesos y se describe cómo cambiar y crear nuevas tablas de decisiones. También se explica la aplicación de reglas.

Correlación de sucesos y aplicación de reglas

Este tema ofrece una visión general del proceso de correlación de sucesos y explica brevemente la aplicación de las reglas.

La aplicación de las reglas de correlación de sucesos basada en WebSphere Operational Decision Management permite modificar y ampliar las reglas de correlación sin conocimientos técnicos avanzados de IBM Intelligent Operations Center or WebSphere Operational Decision Management. Sin embargo, es necesario el conocimiento básico de sucesos de Protocolo Común de Alertas y de WebSphere Operational Decision Management.

Son tres las variables que determinan cómo se correlacionan los sucesos: el suceso de origen, el suceso de destino y la tabla de decisiones.

Para cada suceso de Protocolo Común de Alertas entrante, se llama a la aplicación de las reglas para determinar si alguno de los sucesos existentes se correlaciona con el suceso entrante. El suceso de origen

siempre es el nuevo suceso entrante y desencadena la correlación. El proceso de correlación comprueba el suceso de origen frente a los sucesos de la base de datos. Cuando se encuentra un suceso en la base de datos que se correlaciona con el suceso de origen, este suceso se denomina suceso de destino. Cada vez que se encuentra una posible correlación, el portlet Notificaciones envía una alerta.

La determinación es unidireccional. Este concepto es importante porque las reglas que determinan la correlación no tienen que ser simétrico. Por ejemplo, si el suceso A se correlaciona con el suceso B, no significa que el suceso B se correlaciona con el suceso A.

La aplicación de las reglas proporciona una tabla de correlaciones de muestra que se ajusta a la mayoría de los requisitos. Consulte "Personalización de la configuración de correlación de sucesos" para obtener distintas formas de personalizar las reglas de correlación.

Personalización de la configuración de correlación de sucesos

En esta sección se explica cómo personalizar la configuración de correlación de sucesos.

La tabla de decisiones, que puede editarse en Decision Center, tiene dos tipos de columnas. Las columnas de la izquierda se llaman columnas de decisión. Determinan qué columna de acción, situada a la derecha, se debe utilizar. Las tablas de decisiones se comprueban de izquierda a derecha y, en función de los valores de las distintas filas, conducen a una columna de acción de la derecha. La columna de acción define qué se debe ejecutar cuando se llega a una fila específica.

La forma recomendada para ampliar y modificar la configuración de correlación de sucesos es editar una tabla de decisiones existente. Los siguientes elementos describen cómo se formatean las tablas de decisiones:

- En la parte izquierda de la tabla de decisión (sobre fondo blanco) están las columnas de decisiones. Estas columnas determinan qué filas se ejecutarán de las incluidas en las columnas de acciones (sobre fondo gris).
- La última columna de acción de la tabla llama a la consulta y al servicio de publicación. Si existe una fila de acción que no desea como consulta de correlación y publicación, desactive la entrada en la última columna.
- La columna de consultas SQL en las columnas de acción puede sobrescribir los parámetros de consulta. La sobrescritura de los parámetros de consulta es molesta e innecesaria para la mayoría de las aplicaciones. El requisito para esta consulta es que haya tres columnas designadas en el resultado de la consulta:
  - titular_suceso: el título que se utilizará en la descripción de la correlación. Este texto se convierte en la descripción de la notificación.
  - ID_externo_suceso: el ID externo, como CAP-ID, del suceso
  - ID_interno_suceso: el ID interno, como CapAlertId, que utilizará el portlet Notificaciones para asignar a los titulares en el campo **Se refiere a alertas** de las propiedades de notificación.

Esta sección contiene los temas siguientes:

Modificación de las propiedades de decisión

Utilice la interfaz de usuario de Decision Center en WebSphere Operational Decision Management para cambiar la configuración de la correlación de sucesos. Este tema ofrece más información sobre el cambio de las propiedades de decisión en las tablas de decisiones. También proporciona un vínculo a la documentación de WebSphere Operational Decision Management.

Acerca de esta tarea

La interfaz de usuario se encuentra en el nodo 1 de la instalación de servidor del portal en la siguiente URL: http://*servidor_aplicaciones*:9084/teamserver. Inicie sesión como `waswebadmin`.

La mayoría de los cambios que realice se pueden aplicar dentro de la aplicación de reglas tal como se describe en “Edición de la tabla de decisiones”. Otras modificaciones pueden implicar cambios en:

- Las políticas de Tivoli Netcool/Impact
- El nodo de cálculo de WebSphere Message Broker Java que transforma los mensajes de políticas de impacto a formato bean controlado por mensaje
- Executable Object Model (XOM) de consulta y Business Object Model (BOM)

Para obtener más información e instrucciones para modificar XOM y BOM, información para el nodo de agente de mensajes e información sobre Decision Center, consulte WebSphere Operational Decision Management and WebSphere Message Broker Information Centers utilizando los enlaces siguientes.

Información relacionada:

Information Center de IBM WebSphere Operational Decision Management

Documentación de WebSphere Message Broker

Edición de la tabla de decisiones

Este tema proporciona una breve explicación de la tabla de decisiones y proporciona pasos para cambiar las propiedades de la tabla de decisiones.

En la aplicación de reglas de IBM Intelligent Operations Center WebSphere Operational Decision Management, hay una tabla de correlaciones básicas definida que utiliza la categoría y el tipo del suceso para determinar qué fila de acción se debe ejecutar.

Actualmente, las filas de acción son idénticas, pero puede cambiarlas para ajustarlas a sus necesidades. Por ejemplo, puede definir que los incendios se traten de forma distinta que otros sucesos y sólo se correlacionen con agua y otros incendios. Para cambiar los valores y ajustarlos a sus necesidades, active la celda de la columna Categorías para la fila e introduzca "Incendio, agua" en la celda. Si desea que la regla distinga entre Sucesos e Incidencias, añada una fila a la columna de decisiones y a la columna de acción en consecuencia.

Para cambiar el radio de búsqueda de sucesos correlacionados, cambie el valor **Establecer radio de búsqueda**. El entero introducido se interpreta como metros desde el centro del suceso de origen. Por lo tanto, si introduce `2000`, sólo se correlaciona con sucesos que están a menos de 2000 metros del suceso de origen.

Cambio de las propiedades de la tabla de decisiones

Procedimiento

1. Inicie sesión en http://*servidor_apl*:9084/teamserver como `rtsadmin`.
2. Vaya al explorador del navegador.
3. Pulse **capCorrelationRules**.
4. Pulse **simpleCorrelationPolicy**.
5. Pulse **Editar**. Se mostrará la página de propiedades.
6. Pulse **Siguiente** en la página de propiedades.
7. Edite la tabla. Para consultar ejemplos de columnas que puede añadir a la tabla de decisiones, consulte la plantilla proporcionada en la carpeta de plantillas.
8. Cuando termine de realizar los cambios en la tabla de propiedades, pulse **Finalizar** .

Qué hacer a continuación

Exporte la aplicación de reglas desde Decision Center utilizando el siguiente enlace relacionado.

Tareas relacionadas:

"Despliegue del conjunto de reglas modificado al flujo de IBM Intelligent Operations Center"
Utilice este tema para desplegar el conjunto de reglas modificadas en el servidor de ejecución de reglas

Despliegue del conjunto de reglas modificado al flujo de IBM Intelligent Operations Center

Utilice este tema para desplegar el conjunto de reglas modificadas en el servidor de ejecución de reglas

Acerca de esta tarea

Al modificar las propiedades o los elementos en la tabla de decisiones, debe desplegar el conjunto de reglas modificadas en el flujo de sucesos en IBM Intelligent Operations Center. Después de desplegar el conjunto de reglas modificadas en el servidor de ejecución de reglas, las reglas de correlación funcionarán de forma distinta en función de los cambios. El servidor de ejecución de reglas busca posibles correlaciones en los sucesos entrantes.

Para desplegar el conjunto de reglas modificadas, complete los pasos siguientes.

Procedimiento

1. Exporte la aplicación de reglas desde Decision Center:
   a. Vaya a *servidor_aplicaciones*:9084/teamserver/.
   b. Inicie sesión como rtsadmin.
   c. Vaya a **Proyecto** > **Generar conjunto de reglas**.
   d. Pulse **Siguiente**, no seleccione nada y descargue el archivo jar RuleApp.
2. Importe la aplicación de reglas en el servidor de ejecución de reglas:
   a. Vaya a *servidor_aplicaciones*:9083/res.
   b. Pulse la pestaña Explorador.
   c. Pulse **icoc_wodm_correlation_ruleApp** > **Añadir conjunto de reglas**.
   d. Dé un nombre al conjunto de reglas y anote la vía de acceso del nuevo conjunto de reglas: /icoc_wodm_correlation_ruleApp/1.0/*nombre_elegido*/*versión*.

      Donde
      - *nombre_elegido* es el nombre que ha elegido para el conjunto de reglas
      - *versión* es la versión del conjunto de reglas
3. Establezca la nueva vía de acceso del conjunto de reglas en la política de impacto:
   a. Vaya a event_server:9080/nci/*inicio_sesión_principal*.jsp.
   b. En el menú desplegable de la izquierda, seleccione IBM Intelligent Operations Center.
   c. Pulse **Políticas** y seleccione la política **IOC_Event_Correlation**.
   d. Cambie el valor del campo: **JMSProps.ilog_rules_bres_mdb_rulesetPath** a la nueva vía de acceso: /icoc_wodm_correlation_ruleApp/1.0/*nombre_elegido*/*versión*.

      Donde
      - *nombre_elegido* es el nombre que ha elegido para el conjunto de reglas
      - *versión* es la versión del conjunto de reglas
   e. Pulse **Guardar**.

Tareas relacionadas:

"Cambio de las propiedades de la tabla de decisiones" en la página 179

Gestor de mapas de ubicación

Utilice el portlet Gestor de mapas de ubicación para personalizar el portletMapa de ubicación .

Puede personalizar los siguientes aspectos del portlet Mapa de ubicación :

- Nombre de clasificación que se va a mostrara en el menú a la izquierda del portlet.
- El mapa que se visualizará en el portlet.
- Áreas dentro de un mapa.

Las áreas dentro de un mapa se identifican por medios de códigos de identificador de área. Cualquier suceso con un código identificador de área aparece en todos los mapas de ubicación con dicha área definida.

También hay una opción para brindar a un área un identificador padre. Puede utilizar el identificador padre para crear una jerarquía de áreas. Por ejemplo, crear áreas para representar las tribunas de asientos de la primera planta de un estadio deportivo. Cada zona de asiento se define en el mapa de ubicación detallado del primer piso del estadio. Además, brinde a cada zona de asiento un identificador padre para indicar que se encuentra en el primer piso del estadio. Aparece un suceso con un identificador de área para cada una de las tribuna de asientos en el mapa detallado de asientos de la primera planta. Este suceso también aparece en un mapa general del estadio, ya que el primer piso aquí tiene el mismo identificador de área utilizado como identificador padre para las zonas de asiento.

Para acceder al portlet Gestor de mapas de ubicación, en la interfaz de administración de WebSphere Portal haga clic en **Intelligent Operations** > **Herramientas de personalización** > **Gestor de mapa de ubicaciones**.

Adición de una clasificación al menú del mapa

Utilice la pestaña **Clasificaciones** para añadir una clasificación a mostrar en el menú del mapa del portlet Mapa de ubicación .

Procedimiento

1. Entre un nombre en el campo **Nombre de clasificación** . Tiene la opción de añadir una descripción.
2. Para añadir su clasificación al portlet, haga clic en **Enviar**.

Resultados

La nueva clasificación aparece en el portlet Mapa de ubicación cuando renueva la página del portlet.

Adición de un mapa al portlet

Utilice la pestaña **Mapa de ubicación** para añadir un mapa de ubicación que mostrar en el portlet Mapa de ubicación.

Procedimiento

1. Entre un nombre en el campo **Nombre de clasificación** . Puede seleccionar desde la lista desplegable.
2. Entre un nombre de mapa de ubicación en el campo **Nombre de mapa** . Tiene la opción de añadir una descripción del mapa.
3. Entre una URL para el mapa de ubicación en el campo **Imagen** .
4. Para añadir un mapa al menú, pulse **Enviar**.

Resultados

El mapa aparece en el menú del portlet Mapa de ubicación cuando renueva la página del portlet. Entonces, puede seleccionar y visualizar el mapa.

Añadir o cambiar áreas en un mapa de ubicación

Utilice la pestaña **Áreas** para crear nuevas áreas, cambiar áreas o eliminar áreas para visualización en un mapa de ubicación en el portlet Mapa de ubicación.

Procedimiento

1. Escriba un nombre de mapa en el campo **Nombre de mapa**. Puede seleccionar en la lista desplegable de mapas.
2. Para dibujar un área nueva en el mapa, pulse el símbolo de polígono en la esquina superior derecha del cuadro. Pulse la posición requerida en el mapa y, a continuación, pulse en cada una de las esquinas para dibujar un polígono. Haga doble clic para terminar el polígono. Las nuevas áreas aparecen en verde de forma predeterminada.
3. Para especificar los detalles de un área, haga clic en el símbolo de la mano en la esquina superior derecha del recuadro. Pulse la zona que se va a actualizar.
4. Entre un nombre de mapa de área en el campo **Nombre de área** . Tiene la opción de añadir una descripción.
5. Entre un identificador de área en el campo **Identificador de área** . Tiene la opción de añadir un identificador de área padre.
6. Para actualizar un área en el mapa, pulse **Actualizar área**. Para eliminar un área del mapa, pulse **Eliminar área**.
7. Para añadir los cambios al mapa, haga clic en **Enviar**.

Resultados

Sus cambios aparecen en el portlet Mapa de ubicación al renovar la página del portlet.

Personalización del portlet Gestor de mapas de ubicación

Puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Conceptos relacionados:

"Mapa de ubicación" en la página 282
Utilice el Mapa de ubicación portlet para ver los sucesos marcados en un mapa de ubicación. Un mapa de ubicación en IBM Intelligent Operations Center es un mapa o plano con zonas predefinidas para la interacción, por ejemplo, los asientos en un estadio deportivo.

Referencia relacionada:

"Valores del portlet Gestor de mapas de ubicación" en la página 160
Personalice el portlet Gestor de mapas de ubicación cambiando los valores en los campos de la ventana **Valores compartidos** .

Especificación de datos de configuración de todo el sistema

La tabla de propiedades del sistema IBM Intelligent Operations Center almacena datos de configuración IBM Intelligent Operations Center .

Las siguientes propiedades son propiedades en todo el sistema utilizadas por IBM Intelligent Operations Center.

Tabla 63. Valores de todo el sistema utilizados por IBM Intelligent Operations Center

Dominio	Asunto	Nombre	Tipo	Valor
Sistema	*	ActivityCollectionRefreshInterval	Entero	Velocidad de renovación de la colección en el servidor en segundos. El valor predeterminado es de300 (5 minutos). Esta propiedad afecta a la velocidad del servicio de IU de actualización para las actividades.
Sistema	*	ActivityProviderEJBJNDIName	Serie	El nombre de unión de JNDI de la interfaz remota del proveedor de actividades. A través de esta interfaz, puede desplegar su propio proveedor de actividad para trabar con su proceso o sistema de gestión de flujo de trabajo. El proveedor de actividad es un EJB que implementa la interfaz de actividad en iss_common.jar.
Sistema	*	AppMonitorPort	Serie	Puerto web utilizado por Tivoli Monitoring .
Sistema	*	ApplicationServerHostname	Serie	Nombre de host o dirección IP utilizado por servidor de aplicaciones.
Sistema	*	CollectionRefreshInterval	Entero	Velocidad de renovación de la colección en el servidor en segundos. El valor predeterminado es 15 segundos. Esta propiedad afecta a la velocidad del servicio de IU de actualización para sucesos y notificaciones.
Sistema	*	DatabaseServerHostname	Serie	Nombre de host o dirección IP utilizado por servidor de datos.
Sistema	*	DateFormat	Serie	El formato utilizado cuando IBM Intelligent Operations Center muestra la fecha. El valor predeterminado es aaaa-MM-dd. Se puede especificar cualquier patrón de fecha Java java.text.SimpleDateFormat válido.
Sistema	*	DateTimeFormat	Serie	El formato utilizado cuando IBM Intelligent Operations Center muestra la fecha y hora. El valor predeterminado es aaaa-MM-dd HH:mm:ss. Se puede especificar cualquier patrón de fecha Java java.text.SimpleDateFormat válido.
Sistema	*	DisableTSRMSync	Booleano	Especifica si se ha inhabilitado la sincronización de Tivoli Service Request Manager. El valor predeterminado es "false". Establézcalo en verdadero si el despliegue no contiene la instalación de Tivoli Service Request Manager .

Tabla 63. Valores de todo el sistema utilizados por IBM Intelligent Operations Center (continuación)

Dominio	Asunto	Nombre	Tipo	Valor
Sistema	*	EventContainerDeleteEvent	Serie	Especifica si un suceso se suprime de la base de datos del servidor de objetos de Tivoli Netcool/OMNIbus. La supresión se ha implementado mediante la política de Tivoli Netcool/Impact cuando la base de datos de IBM Intelligent Operations Center se actualiza con un suceso. El valor predeterminado es `true`. Si el valor es `true`, el suceso se borra de la base de datos del servidor de objetos. Si el valor es `false`, el suceso no se borra de la base de datos del servidor de objetos.
Sistema	*	EventRouterPollDelay	Entero	El retraso en milisegundos entre intervalos de sondeo de IU. El retraso es el número de milisegundos antes del siguiente intervalo de sondeo. El valor predeterminado es `0`.
Sistema	*	EventRouterPollErrorDelay	Entero	El retraso en milisegundos entre los intervalos de sondeo de IU después de que se produzca un error. El retraso es el número de milisegundos después de un error y antes del siguiente intervalo de sondeo. El valor predeterminado es `5000`.
Sistema	*	EventRouterTimeout	Entero	El intervalo de sondeo de IU en segundos. El intervalo de sondeo es el intervalo de tiempo durante el cual sondear sucesos antes del tiempo de espera. El valor predeterminado es `20`.
Sistema	*	EventServerHostname	Serie	Nombre de host o dirección IP utilizado por servidor de sucesos.
Sistema	*	MgmtServerHostname	Serie	Nombre de host o dirección IP utilizado por servidor de gestión.
Sistema	*	ModelManagerServerEJBPort	Serie	El puerto de EJB utilizado por servicios de modelo semántico .
Sistema	*	ModelManagerServerHostname	Serie	Nombre de host o dirección IP utilizado por servicios de modelo semántico.
Sistema	*	MonitorServerHostname	Serie	Nombre de host o dirección IP utilizado por IBM WebSphere Business Monitor.
Sistema	*	MonitorServerWebPort	Serie	Puerto web utilizando por IBM WebSphere Business Monitor REST Services Gateway.

Tabla 63. Valores de todo el sistema utilizados por IBM Intelligent Operations Center (continuación)

Dominio	Asunto	Nombre	Tipo	Valor
Sistema	*	MonitorServerSecurityEnabled	Booleano	Especifica si la conexión con IBM WebSphere Business Monitor utiliza SSL para la conexión HTTP segura. El valor predeterminado es `true`. Si el valor es `true`, la conexión utiliza SSL Si el valor es `false`, la conexión no utiliza SSL.
Sistema	*	PortalServerHostname	Serie	Nombre de host o dirección IP utilizado por WebSphere Portal Server.
Sistema	*	PortalServerWebPort	Serie	El puerto web utilizado por WebSphere Portal Server.
Sistema	*	RegExpEmail	Sistema	Expresión regular utilizada para validar una dirección de correo electrónico. El valor predeterminado es `.+`.
Sistema	*	RegExpTelephone	Sistema	Expresión regular utilizada para validar un número de teléfono. El valor predeterminado es `.+`.
Sistema	*	SecurityUserPrefix	Serie	El prefijo de ID de usuario utilizado para correlacionar el usuario con el nombre distinguido LDAP. El valor predeterminado es `uid`.
Sistema	*	SecurityUserSuffix	Serie	Sufijo de ID de usuario utilizado para correlacionar el usuario a otro nombre distinguido LDAP o nombre distinguido local. El valor predeterminado, utilizado al ejecutar un portal con seguridad LDAP, es `ou=users,ou=SWG,o=IBM,c=US`. Establezca el valor en `o=defaultWIMFileBasedRealm` al ejecutar un portal local sin seguridad LDAP.
Sistema	*	TdsPort	Serie	El puerto web utilizado por Tivoli Directory Server Web Administration Tool
Sistema	*	TimeFormat	Serie	Formato utilizado cuando IBM Intelligent Operations Center muestra la hora. El valor predeterminado es `HH:mm:ss`. Se puede especificar cualquier patrón de hora Java `java.text.SimpleDateFormat` válido.
Sistema	*	TSRMDirectServerHostname	Serie	Nombre de host o dirección IP utilizado por Tivoli Service Request Manager.
Sistema	*	TSRMDirectServerWebPort	Serie	Puerto web utilizado por Tivoli Service Request Manager .
Sistema	*	TSRMServerActivityUri	Serie	URI de aplicación de tarea y actividad utilizado por Tivoli Service Request Manager. El valor predeterminado es `/tsrm/maximo/ui/maximo?event=loadapp&value=Activity&uniqueid={0}`. El valor de ID de actividad se sustituye por `{0}`.

Tabla 63. Valores de todo el sistema utilizados por IBM Intelligent Operations Center (continuación)

Dominio	Asunto	Nombre	Tipo	Valor
Sistema	*	TSRMServerResourceAddUri		URI de recurso de adición utilizado por Tivoli Service Request Manager. El valor predeterminado es `/tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additionalevent=INSERT`. El valor de ID de recurso externo se sustituye por `{0}`.
Sistema	*	TSRMServerResourceDeleteUri		URI de recurso de supresión utilizado por Tivoli Service Request Manager. El valor predeterminado es `/tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additionalevent=useqbe&additionaleventvalue=LOCATION={0}`. El valor de ID de recurso externo se sustituye por `{0}`.
Sistema	*	TSRMServerResourcePropertiesUri		URI de propiedades de recurso utilizado por Tivoli Service Request Manager. El valor predeterminado es `/tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additionalevent=useqbe&additionaleventvalue=LOCATION={0}`. El valor de ID de recurso externo se sustituye por `{0}`.
Sistema	*	TSRMServerResourceUpdateUri		URI de recurso de actualización utilizado por Tivoli Service Request Manager. El valor predeterminado es `/tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additionalevent=useqbe&additionaleventvalue=LOCATION={0}`. El valor de ID de recurso externo se sustituye por `{0}`.
Sistema	*	TSRMServerSecurityEnabled	Booleano	Especifica si la conexión HTTP con Tivoli Service Request Manager utilizará SSL. El valor predeterminado es `false`. Si el valor es `true`, la conexión utiliza SSL Si el valor es `false`, la conexión no utiliza SSL.
Sistema	*	TSRMServerWorkflowUri	Serie	URI de flujo de trabajo utilizado por Tivoli Service Request Manager. El valor predeterminado es `/maximo/ui/?event=loadapp&value=sr&&additionalevent=useqbe&additionaleventvalue=TICKETID={0}`. El valor de ID de incidencia se sustituye por `{0}`.

Tabla 63. Valores de todo el sistema utilizados por IBM Intelligent Operations Center (continuación)

Dominio	Asunto	Nombre	Tipo	Valor
Sistema	*	UseDBModelReader	Booleano	Especifica si el modelo de base de datos KPI se lee desde un archivo RDF. El valor predeterminado es `true`. Si el valor es `true`, el modelo KPI no se lee desde un archivo RDF. Si el valor es `false`, el modelo KPI se lee desde un archivo RDF.
Sistema	*	WebSEALServerHostname	Serie	Nombre de host o dirección IP utilizado por Tivoli Access Manager WebSEAL.

Se pueden cambiar las siguientes propiedades para configurar la forma en la que se procesan los KPI.

Tabla 64. Propiedades que afectan el procesamiento de KPI

Dominio	Asunto	Nombre	Tipo	Valor
Indicador clave de rendimiento	*	CacheKpis	Booleano	Especifica si los KPI recuperados desde IBM WebSphere Business Monitor se almacenan en memoria caché. El valor predeterminado es `true`. Si el valor es `true`, los KPI se almacenan en memoria caché para ser reutilizados. ¿Con qué frecuencia `KpiCacheRefreshInterval` especifica la memoria caché renovada? Si el valor es `false`, los KPI se recuperan siempre desde IBM WebSphere Business Monitor cuando IBM Intelligent Operations Center solicita información de KPI.
Indicador clave de rendimiento	*	KpiCacheRefreshInterval	Entero	Especifica la frecuencia con la que se renueva la memoria caché de KPI. El intervalo se especifica en segundos. El valor predeterminado es de`300` (5 minutos). `KPICacheRefreshInterval` se ignora si `CacheKpis` se especifica como `false`.
Indicador clave de rendimiento	*	KpiSentToGroup	Serie	Especifica los grupos que reciben las notificaciones de KPI. Separe los nombres de grupo con un punto y coma (;). El valor predeterminado es `CityWideExecutive;CityWideSupervisor`.

Tabla 64. Propiedades que afectan el procesamiento de KPI (continuación)

Dominio	Asunto	Nombre	Tipo	Valor
Indicador clave de rendimiento	*	PreLoadKpis	Booleano	Especifica si los KPI se recuperan de IBM WebSphere Business Monitor cuando inicia IBM Intelligent Operations Center. El valor predeterminado es `true`. Si es `true`, se recuperan todos los KPI desde IBM WebSphere Business Monitor cuando se inicia IBM Intelligent Operations Center . Los KPI se almacenan en memoria caché para volver a utilizarlos. `KpiCacheRefreshInterval` especifica con qué frecuencia se actualiza la caché. Si es `false`, los KPI se recuperan desde IBM WebSphere Business Monitor solo cuando IBM Intelligent Operations Center solicita información de KPI. **Nota:** Si `PreLoadKpis` es `true`, entonces se supone que`CacheKpis` será `true` independientemente de su valor especificado.

Actualización de la tabla de propiedades del sistema

Para cambiar los datos de configuración de IBM Intelligent Operations Center del sistema, actualice las tablas de propiedades del sistema.

Acerca de esta tarea

Utilice un cliente VNC para iniciar sesión en el servidor de base de datos de servidor de datos y abra una ventana de mandatos. En el siguiente procedimiento, escriba los mandatos en la ventana de mandatos.

Procedimiento

1. Inicie sesión en servidor de datos como raíz
2. Para abrir el Centro de control de DB2®, desactive temporalmente el control de acceso; introduzca los mandatos:

   ```
   xhost +
   su - db2inst1
   db2cc
   ```

3. En el Centro de control de DB2, abra la tabla de propiedades del sistema :
   a. Para abrir el Centro de control de DB2, introduzca el siguiente mandato: `- db2cc`
   b. En el Centro de control de DB2, pulse **Todas las bases de datos** > **IOCDB** > **Tablas** > **SYSPROP**.
   c. Pulse con el botón derecho del ratón en la tabla **SYSPROP** y, a continuación, pulse **Abrir**.
   d. Modifique el campo necesario y pulse **Confirmar**
   e. Cierre la tabla.
4. Cierre el Centro de control de DB2.
5. Para volver al usuario raíz, introduzca el mandato: **`exit`** .
6. Para volver a activar el control de acceso, introduzca el mandato: **`xhost -`**

   Nota: Para implementar los cambios realizados, debe reiniciar el servidor de portal. Puede reiniciar el servidor de portal con el script IOCControl. Para obtener información sobre el inicio de los servicios, consulte el enlace que encontrará al final de este tema.

Tareas relacionadas:

"Inicio de los servicios" en la página 199
Herramienta de control de plataforma está disponible para iniciar los servicios en ejecución en los servidores IBM Intelligent Operations Center.

Configuración de IBM Cognos Business Intelligence para crear informes

IBM Intelligent Operations Center proporciona un subsistema de creación de informes que utiliza IBM Cognos Business Intelligence para crear y gestionar informes. En IBM Intelligent Operations Center se incluye una página de informes que puede mostrar hasta seis informes. También puede crear una página de informes de forma manual y personalizar el diseño de portlet.

El subsistema de creación de informes está instalado en servidor de aplicaciones y utiliza un modelo de datos analítico.

Creación del portlet Informes

Utilice la información de este tema para crear una página de portlet Informes copiando un portlet existente con la consola de IBM Intelligent Operations Center.

Acerca de esta tarea

Para copiar un portlet existente y establecer las propiedades para crear una nueva pagina de informe, complete los pasos siguientes.

Procedimiento

1. Inicie la sesión en IBM Intelligent Operations Center como administrador.
2. Vaya a **Administración** > **Gestión de portlets** > **Portlets**.
3. En el campo **Buscar** , entre `Informes` y pulse **Buscar**. Se visualiza la ventana de portlet Informes.
4. Al lado del portlet que quiere copiar, pulse el icono **Copiar portlet** . Se visualiza la ventana Copiar portlet.
5. Para obtener el nombre del nuevo portlet, entre `CognosReport`.
6. Pulse **Aceptar**. Se visualiza el nuevo portlet en la ventana Gestionar portlet.
7. Vaya a **Administración** > **Interfaz de usuario del portal** > **Gestionar páginas**.
8. Pulse**Raíz de contenido** > **Citywide** y pulse la pestaña **Nueva página** . Se visualiza la página Propiedades de página.
9. Entre las siguientes propiedades para la nueva página de informe:
   a. En el campo **Título** , entre un título para la página de informe. Un título d ejemplo es `Operador: Informes`.
   b. En el campo **Nombre exclusivo** , entre un nombre que identifique específicamente esta página de informe. Un nombre exclusivo de muestra es `com.ibm.iss.ioc.citywide.OperatorReports`.
   c. En el campo **Nombre de URL fácil de usar** , entre `informe`.
   d. En el campo **Tema** , acepte el **Tema padre heredado** predeterminado.
   e. En el campo **Estilo de tema** , acepte la **Política de tema padre heredado** predeterminada.
   f. En **Modalidad Representar-Agregar**, seleccione **Modalidad de representación de padre heredado**.
   g. Pulse **Aceptar**.

   La nueva página de informe se añade a la lista de páginas del portlet.

Edición del diseño de portlet Informes

Utilice estos pasos para dar formato al diseño de la página del portlet Informes.

Acerca de esta tarea

Para seleccionar el diseño de la página del portlet Informes utilizando la consola IBM Intelligent Operations Center , complete los pasos siguientes.

Procedimiento

1. Inicie la sesión en IBM Intelligent Operations Center como administrador.
2. Vaya a **Administración** > **Interfaz de usuario del portal** > **Gestionar páginas**.
3. Al lado de la página que desea editar, pulse el icono **Editar diseño de página** . Se muestra la página Editar diseño.
4. Seleccione el icono de diseño que tiene páginas una al lado de otra con una fila por debajo de las páginas. Este icono es el quinto icono empezando por la izquierda.
5. En el marco donde desea añadir el portlet, pulse **Añadir portlets**.
6. Busque y seleccione la casilla de verificación **CognosPortlet** y pulse **Aceptar** para añadir el portlet al diseño de página. Se muestra un mensaje confirmando que se ha añadido el portlet.
7. Repita los pasos 5 y 6 para añadir portlets adicionales. Puede añadir hasta seis portlets.
8. Pulse **Finalizado**.

Qué hacer a continuación

Puede editar los valores compartidos para cada portlet. En la esquina superior derecha del portlet que desea editar, pulse la flecha y seleccione **Editar valores compartidos** desde el menú. Para obtener más información, consulte “Personalización de un portlet para visualizar los informes”.

Personalización de un portlet para visualizar los informes

Utilice la información de este tema para personalizar un portlet IBM Intelligent Operations Center para visualizar los informes de IBM Cognos Business Intelligence .

Procedimiento

1. Inicie sesión en el portal de la solución como administrador.
2. Seleccione la vista y el portlet que desea personalizar para visualizar los informes.
3. Vaya al menú de visualización de portlet en la esquina superior derecha del portlet.
4. Pulse **Editar valores compartidos**.
5. Entre los valores en los campos proporcionados.
   a. Entre un título para el informe.
   b. Entre la **URL** para el informe. Ubique la URL necesaria como se describe en el tema “Ubicación de la URL de informes” en la página 191.

      ```
      Ejemplo: CAP_events_by_type_status_and_date:
      http://9.161.84.100:9082/ServletGateway/servlet/Gateway?b_action=cognosViewer&ui.action=run
      &ui.object=%2fcontent%2fpackage%5b%40name%3d%27ioc_model%27%5d%2ffolder%5b%40n
      ame%3d%27reports%27%5d%2freport%5b%40name%3d%27CAP_events_by_type_status_and_d
      ate%27%5d&ui.name=CAP_events_by_type_status_and_date&run.outputFormat=&run.prompt=tr
      ue
      ```

   c. Establezca el **Ancho** del portal en *600*.
   d. Establezca la **Altura** del portal en *600*.
   e. Pulse **Guardar**.
   f. En el menú de visualización del portlet, pulse **Atrás** para volver a la vista principal del portlet.

Resultados

El portlet Informes se actualiza para mostrar el informe seleccionado.

Ubicación de la URL de informes

Este tema proporciona los pasos para encontrar la URL para un informe.

Procedimiento

1. Inicie sesión en IBM Cognos Connection.
2. Vaya a **Carpetas públicas** > **ioc_model** > **informes**.
3. Seleccione un informe y pulse el icono **Establecer propiedades** .
4. En la pestaña **General** , pulse **Ver la vía de acceso de búsqueda, ID y URL** para visualizar la URL de informe.
5. En la sección **URL de acción predeterminada** , copie la URL y péguela en el portlet según sea necesario.

Trabajar con el modelo de datos

IBM Intelligent Operations Center ofrece dos modelos de datos que se utilizan al generar informes. Un metamodelo define el idioma y los procesos a partir de los cuales se forma un modelo.

Los informes de IBM Intelligent Operations Center se basan en dos modelos de datos.

- Modelo de datos de esquema común
- Modelo de datos de esquema del protocolo de alertas común (CAP)

Ambos modelos de datos de IBM Intelligent Operations Center están organizados como capas. Para los autores de informe, la capa o vista de presentación está disponible y consta de los siguientes espacios de nombre:

Negocio
: Contiene diccionarios, filtros, y los datos.

Dimensional
: Contiene dimensiones de sucesos para informes y análisis.

Consulta personalizada
: Contiene objetos de consulta que puede utilizar para crear consultas personalizadas para los informes relacionales.

Generación de informes de modelo de datos de esquema común

En este tema se indica cómo generar informes de modelo de datos de esquema común. Estos informes ayudan a los gestores y supervisores a supervisar sucesos actuales, reaccionar antes los sucesos y planificar sucesos futuros.

Acerca de esta tarea

Complete los pasos indicados a continuación haciendo uso de la consola de IBM Intelligent Operations Center para generar informes de modelo de datos de esquema común. Consulte los vínculos de referencia situados al final de este tema para ver una descripción de las opciones disponibles para generar informes.

Procedimiento

1. En la consola de IBM Intelligent Operations Center de la pestaña Administración, haga clic en**Intelligent Operations** > **Herramientas administrativas** > **Consolas de administración**. Se mostrará la página Consolas de administración.
2. En Servidor de aplicaciones, haga clic en **Administración de informes**. Se mostrará la página de IBM Cognos Connection.
3. Haga clic en **ioc common model**. Se mostrarán las carpetas públicas de Cognos.
4. Haga clic en **Informes**.
5. Seleccione el tipo informe que desea generar:

- Para generar un informe de gráfico circular, haga clic en **Gráficos circulares**. Se mostrarán los informes de gráfico circular de esquema común.
- Para generar un informe de gráfico de tabla, haga clic en **Gráficos de tabla**. Se mostrarán los informes de gráfico de tabla de esquema común.

6. Seleccione el informe que desea generar.

Opciones de gráfico circular:

En este tema se describen las opciones que puede seleccionar para generar informes de gráfico circular comunes.

Para acceder a los informes de gráfico circular desde la página de IBM Cognos Connection, haga clic en **Carpetas públicas** > **ioc_common_model** > **informes** > **Gráficos circulares**.

Tabla 65. Opciones de gráfico circular para informes de modelo de datos de esquema común

Informe	Descripción
Suceso por categoría	Muestra sucesos basados en la categoría de suceso. Puede ver, por ejemplo, todos los sucesos medioambientales, incendios o relacionados con el tráfico.
Suceso por certeza	Visualiza sucesos en base a la probabilidad que hay de que sucedan. Por ejemplo, si ha ocurrido un accidente de tráfico, la certeza podría ser "observado".
Suceso por fecha de envío	Este informe muestra los sucesos enviados en una fecha concreta.
Suceso por tipo de suceso	Muestra sucesos basados en tipo. Por ejemplo, el suceso podría ser un tornado que se acerca o un accidente de tráfico.
Suceso por titular	Muestra los sucesos de acuerdo con la descripción especificada para los mismos durante su creación. Así, el titular es en realidad la descripción del suceso.
Suceso por gravedad	Muestra sucesos basados en la gravedad. Por ejemplo, es posible que los sucesos sean extremos o graves.
Suceso por especificación	Muestra los sucesos por especificación. Por ejemplo, un suceso puede ser un suceso dePROTOCOLO Común de Alertas o de Protocolo no común de alertas. Así, este gráfico muestra el porcentaje de sucesos de Protocolo Común de Alertas yProtocolo no común de alertas.
Sucesos por urgencia	Muestra sucesos basados en lo urgentes que son. Por ejemplo, el suceso podría estar ocurriendo y describirse como "inmediato".
Suceso por URL	Muestra los sucesos de acuerdo con el URL especificado para los mismos durante su creación.

Opciones de gráfico de tabla:

En este tema se describe la información que puede generar para los informes de gráfico de tabla comunes.

Para acceder a los informes de gráfico de tabla desde la página de IBM Cognos Connection, haga clic en **Carpetas públicas** > **ioc_common_model** > **informes** > **Gráficos de tabla**.

La única opción de gráfico de tabla disponible para informes de modelo de datos de esquema común es Lista de sucesos. La Lista de sucesos proporciona una lista completa de los sucesos con información detallada de cada uno de ellos. A continuación se explican algunos ejemplos de información de la lista de sucesos.

Tabla 66. Información de lista de sucesos para gráficos de tabla comunes

Campo Informe	Descripción
ID	Identifica el informe
ID de suceso externo	El ID de suceso generado al crear el mismo.
Especificación	Especifica si el suceso es un suceso de Protocolo Común de Alertas o no es un suceso de Protocolo Común de Alertas.
Tipo de suceso	Muestra sucesos basados en tipo. Por ejemplo, el suceso podría ser un tornado que se acerca o un accidente de tráfico.
Enviado	La fecha y hora en que se envió el suceso.
Título	La descripción del suceso.
Categoría	Muestra sucesos basados en la categoría de suceso. Puede ver, por ejemplo, todos los sucesos medioambientales, incendios o relacionados con el tráfico.
Certeza	Visualiza sucesos en base a la probabilidad que hay de que sucedan. Por ejemplo, si ha ocurrido un accidente de tráfico, la certeza podría ser "observado".
Gravedad	Muestra sucesos basados en la gravedad. Por ejemplo, es posible que los sucesos sean extremos o graves.
Urgencia	Muestra sucesos basados en lo urgentes que son. Por ejemplo, el suceso podría estar ocurriendo y describirse como "inmediato".
URL	El URL asociado al informe.

Generación de informes de modelo de datos de esquema de Protocolo Común de Alertas

En este tema se indica cómo generar informes de modelo de datos de esquema de Protocolo Común de Alertas. Estos informes ayudan a los gestores y supervisores a supervisar sucesos actuales, reaccionar antes los sucesos y planificar sucesos futuros.

Acerca de esta tarea

Complete los pasos indicados a continuación haciendo uso de la consola de IBM Intelligent Operations Center para generar informes de modelo de datos de esquema de Protocolo Común de Alertas. Consulte los vínculos de referencia situados al final de este tema para ver una descripción de las opciones disponibles para generar informes.

Procedimiento

1. En la consola de IBM Intelligent Operations Center de la pestaña Administración, haga clic en**Intelligent Operations** > **Herramientas administrativas** > **Consolas de administración**. Se mostrará la página Consolas de administración.
2. En Servidor de aplicaciones, haga clic en **Administración de informes**. Se mostrará la página de IBM Cognos Connection.
3. Haga clic en **ioc cap model**. Se mostrarán las carpetas públicas de Cognos.
4. Haga clic en **Informes**.

5. Seleccione el tipo informe que desea generar:
   - Para generar un informe de modelo de datos indicado en esta página, seleccione el informe.
   - Para generar un informe de gráfico circular, haga clic en **Gráficos circulares**. Se mostrarán los informes de gráfico circular de esquema común.Seleccione el informe en la lista.
   - Para generar un informe definido por el usuario, haga clic en **Informes definidos por el usuario**. Se mostrará la página Informe personalizado de Cognos. Complete los campos del informe personalizado y haga clic en **Actualizar**.

Opciones de informe de modelo de datos:

En este tema se describen las opciones que puede seleccionar para generar un informe deProtocolo Común de Alertas.

Para acceder a las opciones de informe desde la página de IBM Cognos Connection, haga clic en **Carpetas públicas** > **ioc_cap_model** > **informes**.

Tabla 67. Opciones de información sobre informes de Protocolo Común de Alertas

Informe	Descripción
Sucesos de Protocolo Común de Alertas por tipo, estado y fecha	Este informe muestra los sucesos de Protocolo Común de Alertas por tipo, estado o fecha de los mismos. Por ejemplo, el tipo de suceso podría ser "accidente" y el estado "urgente".La fecha podría ser "hoy".
Medidas de KPI de sucesos de Protocolo Común de Alertas por fecha	Este informe muestra sucesos de Protocolo Común de Alertas en base a medidas de KPI de una fecha o rango de fechas particular.
Medidas de KPI de sucesos de Protocolo Común de Alertas por departamento	Este informe muestra sucesos de Protocolo Común de Alertas en base a medidas de KPI de un departamento o área particular. Por ejemplo, el informe podría mostrar medidas de KPI del departamento de aguas o de un área concreta de una ciudad.
Detalles completos de Protocolo Común de Alertas	Este informe muestra detalles completos sobre los sucesos de Protocolo Común de Alertas. Entre los detalles se incluyen, por ejemplo, el ID de Protocolo Común de Alertas, el remitente, la fecha y hora de envío, el estado, el tipo de mensaje, el origen, etc.
Sucesos de IBM Intelligent Operations Center por gravedad de cualquier fecha	Este informe indica todos los sucesos de IBM Intelligent Operations Center en base a su gravedad. Por ejemplo, es posible que los sucesos sean extremos.
Sucesos de IBM Intelligent Operations Center por gravedad en curso	Este informe muestra todos los sucesos de IBM Intelligent Operations Center que están produciéndose actualmente por gravedad. Podría mostrarse, por ejemplo, un suceso climático extremo que se está dando actualmente.

Opciones de gráfico circular:

En este tema se describen las opciones disponibles para generar informes de gráfico circulares deProtocolo Común de Alertas.

Para acceder a los informes de gráfico circular desde la página de IBM Cognos Connection, haga clic en **Carpetas públicas** > **ioc_cap_model** > **informes** > **Gráficos circulares**.

Tabla 68. Opciones de información sobre informes de gráfico circular de Protocolo Común de Alertas

Informe	Descripción
Cobertura por categoría	Muestra Protocolo Común de Alertas por una categoría particular. Puede ver, por ejemplo, todos los sucesos medioambientales, incendios o relacionados con el tráfico.
Cobertura por certeza	Muestra sucesos de Protocolo Común de Alertas basados en la probabilidad de que se produzcan. Por ejemplo, si ha ocurrido un accidente de tráfico, la certeza podría ser "observado".
Cobertura por fecha de envío	Muestra sucesos de Protocolo Común de Alertas enviados en una fecha concreta.
Cobertura por tipo de suceso	Muestra sucesos de Protocolo Común de Alertas en base a su tipo. Por ejemplo, el suceso podría ser un tornado que se acerca o un accidente de tráfico.
Cobertura por código de manejo	Muestra sucesos de Protocolo Común de Alertas por código de manejo. Por ejemplo, el código de manejo podría ser "suceso".
Cobertura por tipo de mensaje	Muestra sucesos de Protocolo Común de Alertas en base a tipos de mensaje, como actualizaciones y alertas.
Cobertura por ámbito	Muestra sucesos de Protocolo Común de Alertas por ámbito. Por ejemplo, un suceso por ámbito podría ser"público".
Cobertura por remitente	Muestra sucesos de Protocolo Común de Alertas por nombre del remitente.
Cobertura por gravedad	Muestra sucesos de Protocolo Común de Alertas en base a su gravedad. Por ejemplo, es posible que los sucesos sean extremos o graves.
Cobertura por origen	Muestra Protocolo Común de Alertas por un origen particular. Por ejemplo, el origen podría ser "transporte".
Cobertura por estado	Muestra sucesos de Protocolo Común de Alertas por estado. Los estados son: • Aceptable • Precaución • Tomar medida
Cobertura por urgencia	Muestra sucesos de Protocolo Común de Alertas en base a su urgencia. Por ejemplo, el suceso podría estar ocurriendo y describirse como "inmediato".
Notificación por categoría	Muestra mensajes de alerta en formato de Protocolo Común de Alertas por una categoría particular. Puede ver, por ejemplo, todos los sucesos medioambientales, incendios o relacionados con el tráfico.
Notificación por tipo	Muestra notificaciones en formato de Protocolo Común de Alertas por tipo. Por ejemplo, el tipo podría ser "actualizaciones" o "alertas".

Opciones de informes de sucesos definidos por el usuario:

En este tema se describen las opciones disponibles para generar informes definidos por el usuario de Protocolo Común de Alertas para los sucesos.

Para acceder a los informes definidos por el usuario desde la página de IBM Cognos Connection, haga clic en **Carpetas públicas** > **ioc_cap_model** > **informes** > **Informes definidos por el usuario** > **Sucesos**.

Tabla 69. Opciones para sucesos de Protocolo Común de Alertas

Informe	Descripción
Sucesos por categoría de cualquier fecha	Muestra todos los sucesos por categoría, independientemente de su fecha. Puede ver, por ejemplo, todos los sucesos medioambientales, incendios o relacionados con el tráfico.
Sucesos por certeza de cualquier fecha	Muestra todos los sucesos por certeza, independientemente de su fecha. Por ejemplo, si ha ocurrido un accidente de tráfico, la certeza podría ser "observado".
Sucesos por tipo de cualquier fecha	Muestra todos los sucesos por tipo, independientemente de su fecha. Por ejemplo, el suceso podría ser un tornado que se acerca o un accidente de tráfico que tuvieran lugar en cualquier momento.
Sucesos por gravedad de cualquier fecha	Muestra todos los sucesos por gravedad, independientemente de su fecha. Por ejemplo, se mostrarán los sucesos extremos o graves de cualquier fecha.
Sucesos por urgencia de cualquier fecha	Muestra todos los sucesos por urgencia, independientemente de su fecha. Por ejemplo, el suceso podría estar ocurriendo y describirse como "inmediato".

Opciones de informe personalizadas definidas por el usuario:

En este tema se describen las opciones disponibles para generar informes personalizados definidos por el usuario de Protocolo Común de Alertas.

Usted puede crear un informe personalizado para sucesos utilizando el portlet de informes. Primero, seleccione cómo desea agrupar sucesos. Por ejemplo, para ver todos los sucesos de una categoría en particular, seleccione **Categoría** en el campo **Agrupar por** . A continuación, en los campos **Seleccionar datos** , elija los datos específicos de la información que desea ver. También puede indicar una fecha o rango de fechas para los sucesos del informe. Pulse **Actualizar**, y el gráfico cambia para reflejar la información que solicitó.

Para recuperar el URL del nuevo informe, haga clic en **URL para este informe**.

Para acceder a los informes personalizados definidos por el usuario desde la página de IBM Cognos Connection, haga clic en **Carpetas públicas** > **ioc_cap_model** > **informes** > **Informes definidos por el usuario** > **Informes definidos por el usuario**.

Tabla 70. Opciones personalizadas definidas por el usuario de Protocolo Común de Alertas

Informe	Descripción
Agrupar por	Seleccione la opción por la que desea agrupar los sucesos.
Gravedad	Muestra sucesos basados en la gravedad. Por ejemplo, es posible que los sucesos sean extremos o graves.
Certeza	Visualiza sucesos en base a la probabilidad que hay de que sucedan. Por ejemplo, si ha ocurrido un accidente de tráfico, la certeza podría ser "observado".

Tabla 70. Opciones personalizadas definidas por el usuario de Protocolo Común de Alertas (continuación)

Informe	Descripción
Urgencia	Muestra sucesos basados en lo urgentes que son. Por ejemplo, el suceso podría estar ocurriendo y describirse como "inmediato".
Categoría de sucesos	Muestra sucesos basados en la categoría de suceso. Puede ver, por ejemplo, todos los sucesos medioambientales, incendios o relacionados con el tráfico.
Tipo de suceso	Muestra sucesos basados en tipo. Por ejemplo, el suceso podría ser un tornado que se acerca o un accidente de tráfico.
Fecha de inicio	Entre la fecha para la que está visualizando sucesos. Para un rango de fechas, introduzca la fecha de inicio.
Fecha final	Entre la fecha a través de la que está visualizando sucesos.

Configuración de informes de modelo de datos de esquema comunes

Utilice este tema para definir las propiedades generales y específicas de los informes de modelo de datos de esquema comunes.

Antes de empezar

Para llevar a cabo este procedimiento debe tener acceso de administrador.

Acerca de esta tarea

Utilice la consola de IBM Intelligent Operations Center para configurar estos informes.

Procedimiento

1. En la consola de IBM Intelligent Operations Center de la pestaña Administración, haga clic en**Intelligent Operations** > **Herramientas administrativas** > **Consolas de administración**. Se mostrará la página Consolas de administración.
2. En Servidor de aplicaciones, haga clic en **Administración de informes**. Se mostrará la página de IBM Cognos Connection.
3. Seleccione la casilla de verificación **ioc common model** y haga clic en **Más**. Se mostrará la página Acciones disponibles.
4. Haga clic en **Establecer propiedades**. Aparecerá la página de las propiedades generales.
5. Seleccione los valores de las propiedades de informe generales.
6. En la pestaña Permisos, seleccione los permisos para los informes de modelo de datos de esquema comunes.
7. En la pestaña Prestaciones, seleccione las prestaciones para los informes.
8. Haga clic en **Aceptar**.

Configuración de informes de modelo de datos de esquema de Protocolo Común de Alertas

Utilice este tema para definir las propiedades generales y permisos, y asignar prestaciones a tipos de usuarios para los informes de modelo de datos de esquema de Protocolo Común de Alertas.

Antes de empezar

Para llevar a cabo este procedimiento debe tener acceso de administrador.

Acerca de esta tarea

Utilice la consola de IBM Intelligent Operations Center para configurar estos informes.

Procedimiento

1. En la consola de IBM Intelligent Operations Center de la pestaña Administración, haga clic en**Intelligent Operations** > **Herramientas administrativas** > **Consolas de administración**. Se mostrará la página Consolas de administración.
2. En Servidor de aplicaciones, haga clic en **Administración de informes**. Se mostrará la página de IBM Cognos Connection.
3. Seleccione la casilla de verificación **ioc cap model** y pulse **Más**. Se mostrará la página Acciones disponibles.
4. Haga clic en **Establecer propiedades**. Aparecerá la página de las propiedades generales.
5. Seleccione los valores de las propiedades de informe generales.
6. En la pestaña Permisos, seleccione los permisos para los informes de modelo de datos de esquema deProtocolo Común de Alertas.
7. En la pestaña Prestaciones, seleccione las prestaciones para los usuarios de los informes.
8. Haga clic en **Aceptar**.

Más opciones para informes

En este tema se describen opciones adicionales para los informes tanto comunes como de Protocolo Común de Alertas.

Para acceder a estas opciones, haga clic en **Más**, situado a la derecha del enlace de un informe particular.

Tabla 71. Opciones adicionales disponibles para cada informe

Opción	Descripción
Definir propiedades	Le permite definir las propiedades generales del informe que desee.
Ver la versión de salida de informe	Elija la versión de salida que desea ver haciendo clic en el hiperenlace de formato.
Ver mis permisos	Visualice los permisos de acceso que tiene para esta entrada.
Ejecutar con opciones	Seleccione cómo desea ejecutar y recibir el informe. Entre los ejemplos se incluyen HTML y PDF.
Abrir en Report Studio	Muestra el informe en otro navegador utilizando Report Studio.
Abrir con Business Insight Advanced	Muestra el informe en otro navegador utilizando IBM Cognos Business Insight Advanced.
Nueva planificación	Planifica un informe basándose en diversos criterios.
Mover	Mueve un informe a una ubicación diferente.
Copiar	Copia un informe de una ubicación a otra.
Crear un acceso directo a esta entrada	Crea un acceso directo para acceder al informe en su escritorio.
Crear una vista de informe de este informe	Crea una vista de este informe en su escritorio almacenada en un directorio local.
Suprimir	Suprime un informe mostrado.

Capítulo 6. Gestión de la solución

Los temas de esta sección describen cómo realizar tareas administrativas para IBM Intelligent Operations Center.

Acerca de

Utilice el portlet Acerca de para ver detalles de la versión del IBM Intelligent Operations Center y el IBM Smarter Cities Software Solutions integrado que ha instalado. También puede ver detalles de las actualizaciones que aplicó desde la instalación.

Para iniciar el portlet Acerca de, en la interfaz de administración de WebSphere Portal haga clic en **Intelligent Operations** > **Acerca de**.

El portlet Acerca de proporciona la siguiente información:
- La ubicación de todos los productos de software y componentes instalados.
- El nombre y la versión de los productos instalados.
- El nombre y la versión de los componentes instalados.
- Los detalles de cualquier arreglo aplicado.

Los componentes que se identifican son componentes o partes de un producto, por ejemplo:
- Una parte de un producto que tiene una corriente de servicio o mantenimiento dedicada.
- Una parte opcionalmente instalable de un producto
- Partes de un producto compartido por múltiples productos

Nota: La información mostrada para cada arreglo depende de la terminación del paso adecuado en las instrucciones de instalación proporcionadas por ese arreglo.

Personalización del portlet Acerca de

Puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Tareas relacionadas:

"Verificación de la instalación" en la página 52
Después de instalar IBM Intelligent Operations Center, verifique que el producto se ha instalado correctamente.

Referencia relacionada:

"Valores del portlet Acerca de" en la página 150
Personalice el portlet Acerca de cambiando los valores en los campos de la ventana **Valores compartidos** .

Control de los servicios

Los servicios IBM Intelligent Operations Center que se ejecutan en los servidores IBM Intelligent Operations Center se pueden controlar y consultar.

Inicio de los servicios

Herramienta de control de plataforma está disponible para iniciar los servicios en ejecución en los servidores IBM Intelligent Operations Center.

Acerca de esta tarea

El mandato **IOCControl.sh** se debe ejecutar como el usuario ibmadmin. Si no ha iniciado sesión como ibmadmin , ejecute el mandato **su - ibmadmin** para cambiar al usuario ibmadmin.

Atención: El inicio de los servicios individuales sólo deben realizarlo administradores de IBM Intelligent Operations Center experimentados. Pueden producirse resultados impredecibles si los servicios no se inician en el orden requerido.

Procedimiento

En servidor de gestión ejecute el mandato siguiente para iniciar todos los servicios de IBM Intelligent Operations Center.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh iniciar todos contraseña
```

donde *contraseña* es la contraseña de Herramienta de control de plataforma definida cuando se ha instalado Herramienta de control de plataforma.
Los servicios se han iniciado en el orden requerido. Los servicios de los requisitos previos se han iniciado antes que los servicios dependientes. Por ejemplo, los servicios de base de datos y directorio se han iniciado en primer lugar.
Para iniciar sólo el servicio, ejecute el mandato siguiente.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start ID_servicio contraseña
```

donde *ID_servicio* es un ID listado en **Opciones de destino** en la ayuda de **IOCControl** y donde *contraseña* es la contraseña de Herramienta de control de plataforma definida cuando se ha instalado Herramienta de control de plataforma.

Resultados

Se han iniciado los servicios de IBM Intelligent Operations Center solicitados.

Qué hacer a continuación

Tras ejecutar el mandato **IOCControl.sh**, compruebe los registros en el directorio /opt/IBM/ISP/mgmt/logs. Los registros contienen los resultados del mandato **IOCControl.sh**.

Tareas relacionadas:

"Detención de los servicios" en la página 203
Herramienta de control de plataforma está disponible para detener los servicios de IBM Intelligent Operations Center.

"Consulta del estado de los servicios" en la página 206
Herramienta de control de plataforma está disponible para determinar el estado de los servicios de IBM Intelligent Operations Center.

"Obtención de ayuda para Herramienta de control de plataforma" en la página 207
Existe información disponible sobre las opciones de acción y objetivo para Herramienta de control de plataforma.

"Verificación de la instalación" en la página 52
Después de instalar IBM Intelligent Operations Center, verifique que el producto se ha instalado correctamente.

"Instalación de Herramienta de control de plataforma" en la página 49
El Herramienta de control de plataforma se utiliza para gestionar el entorno de servidor de IBM Intelligent Operations Center . La herramienta se instalada independiente del producto.

"Instalación de la herramienta Comprobación de verificación del sistema" en la página 50
La herramienta Comprobación de verificación del sistema se utiliza para verificar el estado operativo de los componentes en IBM Intelligent Operations Center. La herramienta se instalada independiente del producto.

Orden de inicio necesario

Los servicios de IBM Intelligent Operations Center se deben iniciar en un orden específico.

Herramienta de control de plataforma se utiliza para iniciar los servicios de IBM Intelligent Operations Center. Aunque se recomienda utilizar la opción Herramienta de control de plataforma **`iniciar todo`** para iniciar todos los servicios, puede que haya veces que se tengan que iniciar servicios individuales.

Algunos servicios tienen dependencias en otros servicios, así que deben iniciarse en un orden específico.

En general, los servicios se deben iniciar en tres grupos:

Grupo 1
`tds`, `db24po`, `db24sms`, `db24wbm`, `db24ana`, `db24tsrm`, `db24sol`, `db24mgmt`

Grupo 2
`ihs`, `appdmgr`, `st`

Grupo 3
todos los servicios restantes

Inicie los servicios del grupo 1 primero, a continuación el grupo 2 y, por último, el grupo 3. Los servicios de cada grupo se pueden iniciar en cualquier orden.

Tabla 72. Dependencias de orden de inicio del servicio IBM Intelligent Operations Center

Servicio	Descripción	Servicios que se deben ejecutar antes de iniciar este servicio
`db24po`	DB2 Enterprise Server Edition para WebSphere Portal Server	Ninguno
`db24wbm`	DB2 Enterprise Server Edition para WebSphere Business Modeler	Ninguno
`db24sol`	DB2 Enterprise Server Edition para IBM Intelligent Operations Center	Ninguno
`db24ana`	DB2 Enterprise Server Edition para Cognos	Ninguno

Tabla 72. Dependencias de orden de inicio del servicio IBM Intelligent Operations Center (continuación)

Servicio	Descripción	Servicios que se deben ejecutar antes de iniciar este servicio
db24mgmt	DB2 Enterprise Server Edition para servicios de Tivoli Enterprise Portal	Ninguno
db24tsrm	DB2 Enterprise Server para Tivoli Service Request Manager	Ninguno
db24sms	DB2 Enterprise Server para servicios de modelo semántico	Ninguno
tds	Tivoli Directory Server	Ninguno
tdspxyapp	Proxy Tivoli Directory Server (servidor de aplicaciones)	tds
tdspxyevt	Proxy Tivoli Directory Server (servidor de sucesos)	tds
tdspxymgt	Proxy Tivoli Directory Server (servidor de gestión)	tds
tdsappsrv	Servidor de aplicaciones Tivoli Directory Server	Ninguno
tamps	Servidor de políticas Tivoli Access Manager	tamas
tamas	Servidor de autorización Tivoli Access Manager	tds
tamwpm	Gestor de portal web Tivoli Access Manager	Ninguno
tamweb	Tivoli Access Manager WebSEAL	tamas
tems	Tivoli Monitoring Enterprise Monitoring Server	Ninguno
teps	Tivoli Monitoring Enterprise Portal Server	tems, db24mgmt
tim	Tivoli Identity Manager	tds
appdmgr	WebSphere Application Server Network Deployment	Ninguno
cplex	WebSphere Application Server para CPLEX	db24sms
ihs	HTTP Server for Runtime (servidor de aplicaciones)	Ninguno
ihsevt	HTTP Server for Runtime (servidor de sucesos)	ihs
ihsmgt	HTTP Server for Runtime (servidor de gestión)	ihs
ncob	Tivoli Netcool/OMNIbus	Ninguno
nci	Tivoli Netcool/Impact	ncob
wbm	IBM WebSphere Business Monitor	db24wbm
st	Lotus Sametime	Ninguno
stpxy	Servidor de aplicación Lotus Sametime Proxy	st
wpe	WebSphere Portal Extend	tdspxyapp, db24po, appdmgr
wmb	WebSphere Message Broker	Ninguno
cognos	IBM Cognos Business Intelligence	db24ana, appdmgr
tsrm	Tivoli Service Request Manager	appdmgr, db24tsrm
wodm	WebSphere Operations Decision Manager	appdmgr
wodmdc	WebSphere Operations Decision Manager (Decision Center)	Ninguno
smsclt	Servicios de modelo semántico (servicios de cliente)	appdmgr
smsdaaq	Servicios de modelo semántico (Servicios de datos)	appdmgr
smsmdl	Servicios de modelo semántico (servicios de modelo)	appdmgr
smsmgmt	Servicios de modelo semántico (servicios de gestión)	appdmgr
smsrtc	Servicios de modelo semántico (servicios de RTC)	appdmgr
iocxml	Analizador XML de IBM Intelligent Operations Center	db24sol

Inicio y detención del analizador Tivoli Netcool/OMNIbus

Inicie el analizador Tivoli Netcool/OMNIbus una vez se hayan iniciado todos los servidoresIBM Intelligent Operations Center .

Acerca de esta tarea

El analizador forma parte del script `IOCControl`. El analizador ha iniciado y se ha detenido al iniciar y detener Tivoli Netcool/OMNIbus. El analizador Tivoli Netcool/OMNIbus está enlazado con Tivoli Netcool/OMNIbus en el script. Utilice el siguiente procedimiento para detener, iniciar y verificar el estado del analizador.

Procedimiento

1. Para detener el analizador, en servidor de gestión ejecute:
   ```
   /opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop ncob password
   ```
2. Para iniciar el analizador, en servidor de gestión ejecute:
   ```
   /opt/IBM/ISP/mgmt/scripts/IOCControl.sh start ncob password
   ```
3. Para verificar el estado del analizador:
   - En servidor de gestión, ejecute el mandato:
     ```
     /opt/IBM/ISP/mgmt/scripts/IOCControl.sh start iocxml password
     ```
   - En servidor de sucesos, ejecute el mandato:
     ```
     tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
     ```

Detención de los servicios

Herramienta de control de plataforma está disponible para detener los servicios de IBM Intelligent Operations Center.

Acerca de esta tarea

El mandato **`IOCControl.sh`** se debe ejecutar como el usuario `ibmadmin`. Si no ha iniciado sesión como `ibmadmin` , ejecute el mandato **`su - ibmadmin`** para cambiar al usuario `ibmadmin`.

Atención: Sólo se deben encargar de la detención de servicios individuales los administradores de IBM Intelligent Operations Center más experimentados. Se pueden producir resultados impredecibles si los servicios no se detienen en el orden deseado.

Procedimiento

En servidor de gestión ejecute el mandato siguiente para detener todos los servicios de IBM Intelligent Operations Center.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh detener todo contraseña
```

donde *contraseña* es la contraseña de Herramienta de control de plataforma definida cuando se ha instalado Herramienta de control de plataforma.
Para detener sólo un servicio, ejecute el mandato siguiente.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop ID_servicio contraseña
```

donde *ID_servicio* es un ID listado en **Opciones de destino** en la ayuda de **`IOCControl`** y donde *contraseña* es la contraseña de Herramienta de control de plataforma definida cuando se ha instalado Herramienta de control de plataforma.

Resultados

Los servicios de IBM Intelligent Operations Center solicitados se han detenido.

Qué hacer a continuación

Tras ejecutar el mandato **IOCControl.sh**, compruebe los registros en el directorio /opt/IBM/ISP/mgmt/logs. Los registros contienen los resultados del mandato **IOCControl.sh**.

Tareas relacionadas:

"Inicio de los servicios" en la página 199
Herramienta de control de plataforma está disponible para iniciar los servicios en ejecución en los servidores IBM Intelligent Operations Center.

"Consulta del estado de los servicios" en la página 206
Herramienta de control de plataforma está disponible para determinar el estado de los servicios de IBM Intelligent Operations Center.

"Obtención de ayuda para Herramienta de control de plataforma" en la página 207
Existe información disponible sobre las opciones de acción y objetivo para Herramienta de control de plataforma.

"Verificación de la instalación" en la página 52
Después de instalar IBM Intelligent Operations Center, verifique que el producto se ha instalado correctamente.

"Instalación de Herramienta de control de plataforma" en la página 49
El Herramienta de control de plataforma se utiliza para gestionar el entorno de servidor de IBM Intelligent Operations Center . La herramienta se instalada independiente del producto.

"Instalación de la herramienta Comprobación de verificación del sistema" en la página 50
La herramienta Comprobación de verificación del sistema se utiliza para verificar el estado operativo de los componentes en IBM Intelligent Operations Center. La herramienta se instalada independiente del producto.

Orden de detención necesaria

Los servicios de IBM Intelligent Operations Center se deben detener en un orden específico.

Herramienta de control de plataforma se utiliza para detener los servicios de IBM Intelligent Operations Center. Aunque se recomienda utilizar la opción Herramienta de control de plataforma **detener todo** para detener todos los servicios, puede que haya veces que se tengan que detener servicios individuales.

Algunos servicios tienen dependencias en otros servicios, así que deben detenerse en un orden específico.

En general, los servicios se deben detener en tres grupos:

Grupo 1
tds, db24po, db24sms, db24wbm, db24ana, db24tsrm, db24sol, db24mgmt

Grupo 2
ihs, appdmgr, st

Grupo 3
todos los servicios restantes

Detenga primero los servicios del grupo 3, después los del grupo 2 y, finalmente, los servicios del grupo 1. Los servicios dentro de cada grupo se pueden detener en cualquier orden.

Tabla 73. Dependencias de orden de detención del servicio IBM Intelligent Operations Center

Servicio	Descripción	Servicios que se deben detener antes de detener este servicio
db24po	DB2 Enterprise Server Edition para WebSphere Portal Server	wpe

Tabla 73. Dependencias de orden de detención del servicio IBM Intelligent Operations Center (continuación)

Servicio	Descripción	Servicios que se deben detener antes de detener este servicio
db24wbm	DB2 Enterprise Server Edition para WebSphere Business Modeler	wbm
db24sol	DB2 Enterprise Server Edition para IBM Intelligent Operations Center	iocxml
db24ana	DB2 Enterprise Server Edition para Cognos	cognos
db24mgmt	DB2 Enterprise Server Edition para servicios de Tivoli Enterprise Portal	teps
db24tsrm	DB2 Enterprise Server para Tivoli Service Request Manager	tsrm
db24sms	DB2 Enterprise Server para servicios de modelo semántico	cplex
tds	Tivoli Directory Server	tdsprxyapp, tdspxyevt, tdspxymgt, tamas, tim
tdspxyapp	Proxy Tivoli Directory Server (servidor de aplicaciones)	wpe
tdspxyevt	Proxy Tivoli Directory Server (servidor de sucesos)	Ninguno
tdspxymgt	Proxy Tivoli Directory Server (servidor de gestión)	Ninguno
tdsappsrv	Servidor de aplicaciones Tivoli Directory Server	Ninguno
tamps	Servidor de políticas Tivoli Access Manager	Ninguno
tamas	Servidor de autorización Tivoli Access Manager	tamps
tamwpm	Gestor de portal web Tivoli Access Manager	Ninguno
tamweb	Tivoli Access Manager WebSEAL	Ninguno
tems	Tivoli Monitoring Enterprise Monitoring Server	teps
teps	Tivoli Monitoring Enterprise Portal Server	Ninguno
tim	Tivoli Identity Manager	Ninguno
appdmgr	WebSphere Application Server Network Deployment	wpe, cognos, tsrm, wodm, smsclt, smsdaaq, smsmdl, smsrtc, smsmgmt
cplex	WebSphere Application Server para CPLEX	Ninguno
ihs	HTTP Server for Runtime (servidor de aplicaciones)	ihsevt, ihsmgt
ihsevt	HTTP Server for Runtime (servidor de sucesos)	Ninguno
ihsmgt	HTTP Server for Runtime (servidor de gestión)	Ninguno
ncob	Tivoli Netcool/OMNIbus	nci
nci	Tivoli Netcool/Impact	Ninguno
wbm	IBM WebSphere Business Monitor	Ninguno
st	Lotus Sametime	stpxy
stpxy	Servidor de aplicación Lotus Sametime Proxy	Ninguno
wpe	WebSphere Portal Extend	Ninguno
wmb	WebSphere Message Broker	Ninguno
cognos	IBM Cognos Business Intelligence	Ninguno
tsrm	Tivoli Service Request Manager	Ninguno
wodm	WebSphere Operations Decision Manager	Ninguno
wodmdc	WebSphere Operations Decision Manager (Decision Center)	Ninguno

Tabla 73. Dependencias de orden de detención del servicio IBM Intelligent Operations Center (continuación)

Servicio	Descripción	Servicios que se deben detener antes de detener este servicio
smsclt	Servicios de modelo semántico (servicios de cliente)	Ninguno
smsdaaq	Servicios de modelo semántico (Servicios de datos)	Ninguno
smsmdl	Servicios de modelo semántico (servicios de modelo)	Ninguno
smsmgmt	Servicios de modelo semántico (servicios de gestión)	Ninguno
smsrtc	Servicios de modelo semántico (servicios de RTC)	Ninguno
iocxml	Analizador XML de IBM Intelligent Operations Center	Ninguno

Consulta del estado de los servicios

Herramienta de control de plataforma está disponible para determinar el estado de los servicios de IBM Intelligent Operations Center.

Acerca de esta tarea

El mandato **IOCControl.sh** se debe ejecutar como el usuario ibmadmin. Si no ha iniciado sesión como ibmadmin , ejecute el mandato **su - ibmadmin** para cambiar al usuario ibmadmin.

Procedimiento

En servidor de gestión, ejecute el mandato siguiente para consultar el estado de todos los servicios de IBM Intelligent Operations Center.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh estado todos contraseña
```

donde *contraseña* es la contraseña de Herramienta de control de plataforma definida cuando se ha instalado Herramienta de control de plataforma.
Para comprobar sólo un servicio, ejecute el mandato siguiente.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status ID_servicio contraseña
```

donde *ID_servicio* es un ID listado en **Opciones de destino** en la ayuda de **IOCControl** y donde *contraseña* es la contraseña de Herramienta de control de plataforma definida cuando se ha instalado Herramienta de control de plataforma.

Resultados

Los servicios que se han iniciado mostrarán **[on]**. Los servicios que no se han iniciado mostrarán **[off]**.

Qué hacer a continuación

Tras ejecutar el mandato **IOCControl.sh**, compruebe los registros en el directorio /opt/IBM/ISP/mgmt/logs. Los registros contienen los resultados del mandato **IOCControl.sh**.

Tareas relacionadas:

"Inicio de los servicios" en la página 199
Herramienta de control de plataforma está disponible para iniciar los servicios en ejecución en los servidores IBM Intelligent Operations Center.

"Detención de los servicios" en la página 203
Herramienta de control de plataforma está disponible para detener los servicios de IBM Intelligent Operations Center.

"Obtención de ayuda para Herramienta de control de plataforma"
Existe información disponible sobre las opciones de acción y objetivo para Herramienta de control de plataforma.

"Instalación de Herramienta de control de plataforma" en la página 49
El Herramienta de control de plataforma se utiliza para gestionar el entorno de servidor de IBM Intelligent Operations Center . La herramienta se instalada independiente del producto.

Obtención de ayuda para Herramienta de control de plataforma

Existe información disponible sobre las opciones de acción y objetivo para Herramienta de control de plataforma.

Acerca de esta tarea

El mandato **IOCControl.sh** se debe ejecutar como el usuario `ibmadmin`. Si no ha iniciado sesión como `ibmadmin` , ejecute el mandato **su - ibmadmin** para cambiar al usuario `ibmadmin`.

Procedimiento

En servidor de gestión ejecute uno de los siguientes mandatos para ver las opciones para el mandato **IOCControl** .

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh help
```

o

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh
```

Resultados

Se visualizan las opciones para el mandato **IOCControl** .

Tareas relacionadas:

"Inicio de los servicios" en la página 199
Herramienta de control de plataforma está disponible para iniciar los servicios en ejecución en los servidores IBM Intelligent Operations Center.

"Detención de los servicios" en la página 203
Herramienta de control de plataforma está disponible para detener los servicios de IBM Intelligent Operations Center.

"Consulta del estado de los servicios" en la página 206
Herramienta de control de plataforma está disponible para determinar el estado de los servicios de IBM Intelligent Operations Center.

Consolas de administración

Utilice el portlet Consolas de administración para administrar los servicios proporcionados por la solución.

Para acceder al portlet Consolas de administración, en la interfaz de administración de WebSphere Portal haga clic en **Intelligent Operations** > **Herramientas de administración** > **Consolas de administración**.

Para cada servicio, los enlaces del portlet Consolas de administración le dirigen a una consola de administración o a información sobre cómo acceder a la administración.

Nota: Si está utilizando Microsoft Internet Explorer versión 8.0, es posible que se encuentre un problema con el enlace de administración de informes. El mensaje es: `No se puede encontrar el recurso solicitado`. La solución es editar la dirección URL en el campo de dirección del navegador añadiendo, `/cognos`, entre el nombre de host y `/ServletGateway`.

Servidor de aplicaciones

Tabla 74. Administración en el servidor de aplicaciones

Consola	Administración
Servidor de aplicaciones	Para administrar varios servicios que proporciona el IBM Intelligent Operations Center, utilice el enlace a la consola basada en web para WebSphere Application Server. Puede controlar los servidores, gestionar recursos y proveedores de servicio, cambiar el host y otros valores del entorno.
Administración de informes	Para establecer informes, utilice el enlace a la consola basada en la web para IBM Cognos Connection . Puede crear nuevos informes o modificar los existentes. También puede configurar orígenes de datos, establecer carpetas públicas y privadas, definir permisos y distribución y planificar informes para que se ejecuten automáticamente.

Servidor de datos

Tabla 75. Administración en el servidor de datos

Consola	Administración
Base de datos	Para obtener detalles sobre cómo administrar la base de datos con DB2 Enterprise Server Edition, utilice el enlace al Information Center. Puede realizar tareas con la GUI del centro de control de base de datos o la línea de mandatos.

Servidor de sucesos

Tabla 76. Administración en el servidor de sucesos

Consola	Administración
Contactos	Para ver los valores actuales en la base de datos names.nsf, utilice el enlace a la consola basada en la web para Lotus Domino Server. names.nsf se utiliza para configurar Lotus Domino Server. Los cambios de configuración se realizan con Domino Administration Client.
Administración de contactos	Para obtener detalles sobre cómo descargar y establecer Domino Administration Client para la administración de contactos de Lotus Domino , utilice el enlace al Information Center.
Manejo de sucesos	Para administrar el manejo de sucesos con la GUI del servidor de objetos, utilice el enlace a la consola basada en web para Tivoli Netcool/OMNIbus.

Tabla 76. Administración en el servidor de sucesos (continuación)

Consola	Administración
Proceso y mejora de sucesos	Para administrar el procesamiento de sucesos, utilice el enlace a la consola basada en la web para Tivoli Netcool/Impact. Por ejemplo, puede comprobar las conexiones a base de datos, las conexiones de origen de datos, la iniciación del proceso de sucesos, estado de políticas y registros.
Servidor de mensajería instantánea	Para administrar la mensajería instantánea, utilice el enlace a la consola basada en web para Lotus Sametime Community Server.
Bus de mensajería	Para obtener detalles sobre cómo comprobar el estado de los mensajes conWebSphere Message Broker, utilice el enlace al Information Center.
Administración de Procedimiento operativo estándar	Para definir recursos y procedimientos de operación estándar, utilice el enlace a la consola basada en la web para Tivoli Service Request Manager Start Center. Puede definir recursos y actividades disponibles para la gestión de sucesos en IBM Intelligent Operations Center.
Servidor de aplicaciones Procedimiento operativo estándar	Para administrar, utilice el enlace a la consola basada en web para WebSphere Application Server que proporciona Tivoli Service Request Manager.

Servidor de gestión

Tabla 77. Administración en el servidor de gestión

Consola	Administración
Supervisión de aplicaciones	Para administrar la supervisión de aplicaciones, utilice el enlace a la consola basada en web para Tivoli Monitoring. Puede trabajar con esta consola para comprobar el estado del sistema.
Servidor de aplicación para la gestión	Para administrar aplicaciones integradas, utilice el enlace a la consola basada en la web para WebSphere Application Server. Esta administración incluye la administración de seguridad con Tivoli Access Manager y WebSEAL.
Base de datos	Para obtener detalles sobre cómo administrar la base de datos con DB2 Enterprise Server Edition, utilice el enlace al Information Center. Puede realizar tareas con la GUI del centro de control de base de datos o la línea de mandatos.
Directorio	Para administrar el directorio de usuario, utilice el enlace a la consola basada en la web para Tivoli Directory Server .Para obtener más detalles sobre cómo utilizar la consola web deTivoli Directory Server, utilice el enlace al Information Center.

Personalización del portlet Consolas de administración

Puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Referencia relacionada:

"Valores del portlet Consolas de administración" en la página 150
Personalice el portlet Consolas de administración cambiando los valores en los campos de la ventana **Valores compartidos** .

Información relacionada:

IBM Lotus Domino and Notes information center

IBM DB2 Database information center

IBM Tivoli Directory Server information center

Gestión de servicios

El portlet de Consolas de administración proporciona enlaces a ubicaciones donde puede gestionar los servicios proporcionados por la solución o buscar información más detallada sobre la gestión de servicios.

Servidor de aplicaciones

Servicio del servidor de aplicaciones

Puede realizar una gran variedad de tareas de gestión de aplicaciones en Integrated Solutions Console, una consola basada en web común:

- Comprobar el estado de los servidores.
- Iniciar y detener servidores y clústeres.
- Desplegar aplicaciones o parches.
- Gestionar la lista de portlets disponibles.
- Supervisar los servicios.
- Trabajar con políticas de servicios de aplicaciones.
- Gestionar proveedores de servicios, como proveedores de servicio REST.
- Gestionar recursos.
- Gestionar la seguridad de las aplicaciones.
- Trabajar con hosts virtuales y otra configuración de entorno.
- Administrar el sistema.
- Gestionar la integración de servicio.
- Administrar el servidor HTTP.
- Gestionar registros y rastreos.

Para obtener más información sobre el servicio de aplicación, consulte la ayuda en línea de Integrated Solutions Console o el enlace al centro de información de WebSphere Application Server que encontrará al final de la sección de servidor de aplicaciones.

Servicio de administración de informes

Para todas las tareas asociadas con el suministro de informes en IBM Intelligent Operations Center, puede utilizar la consola de administración de informes basada en web:

- Configurar orígenes de datos.
- Crear, editar y suprimir informes.
- Gestionar acceso a los informes.
- Planificar informes.
- Configurar la distribución de informes.

Para obtener más información sobre el servicio de administración de informes, consulte el enlace a IBM Cognos Business Intelligence Information Center al final de la sección de servidor de aplicaciones.

Información relacionada:

WebSphere Application Server Version 7.0 information center

IBM Cognos Business Intelligence information center

Servidor de datos

Servicio de base de datos

Puede gestionar las bases de datos de IBM Intelligent Operations Center a través de las instancias de servicio de base de datos alojadas en servidor de datos. Una instancia de servicio de base de datos es un proceso separado e independiente que se ejecuta en un servidor. Una instancia puede alojar varias bases de datos. Cada instancia tiene un nombre *nombre-instancia*. Las instancias siguientes se alojan en el servidor de datos:

Tabla 78. Instancias de base de datos alojadas en servidor de datos

Instancia	Utilizada por
dsrdbm01	servicio de directorio
db2inst1	reservado para soluciones
db2inst2	servidor del portal
db2inst3	administración de informes
db2inst4	reglas de negocio y servicio de supervisión empresarial
db2inst5	servicios de modelo semántico
db2inst6	servicio de administración de procedimiento operativo estándar
db2inst7	servicio de gestión de identidad
db2inst8	reservado para aplicaciones

Para administrar una instancia desde una ventana terminal:

1. Inicie sesión como el usuario *nombre-instancia*.
2. Ejecute el mandato **db2** para introducir el modo de mandato.
3. Introduzca **?** para ver una lista de mandatos disponibles. Muchos mandatos requieren una conexión activa a una base de datos.
   - Para ver las bases de datos disponibles para una instancia, ejecute el mandato **list database directory** .
   - Para conectarse a una base de datos, ejecute el mandato **connect to** *nombre_base_datos*.
4. Para desconectarse de una base de datos y finalizar el modo de mandato solicitado, ejecute el mandato **terminate**.

Para obtener más información sobre el servicio de base de datos, consulte el enlace con DB2 Database Information Center al final de la sección de servidor de datos.

Información relacionada:

IBM DB2 Database information center

Servidor de sucesos

Contactos, administración de contactos y servicios de mensajería instantánea

Puede gestionar contactos, administración de contactos y servicios de mensajería instantánea a través de:

- Consola de servidor Lotus Domino para ver los contactos actuales.
- Cliente de administración de Lotus Domino para configurar el inicio de sesión único, administrar el servidor de mensajería instantánea y Lotus Sametime Client.
- Lotus Sametime Community Server para registrar y comprobar la disponibilidad del servidor de mensajería instantánea.

Nota: Los contactos que se ven en la consola de servidor de Lotus Domino se aplican sólo al portlet de Contactos y no son los mismos que los usuarios de IBM Intelligent Operations Center.

Para obtener más información sobre los servicios de contactos, administración de contactos y mensajería instantánea, consulte el enlace con el centro de información de Lotus Domino y Notes al final de la sección de servidor de sucesos.

Servicio de gestión de sucesos

Puede gestionar la captura de sucesos y el almacenamiento en IBM Intelligent Operations Center a través de la GUI del servidor de objetos Tivoli Netcool/OMNIbus.

1. Abra una sesión de terminal habilitada del sistema X Window.
2. Inicie sesión como raíz en el servidor.
3. Vaya al directorio `/opt/IBM/netcool/omnibus`.
4. Para abrir la aplicación GUI, ejecute el mandato: `bin/nco_config`

Para obtener más información sobre el servicio manejo de sucesos, consulte el enlace al centro de información de Tivoli Netcool/Impact al final de la sección de servidor de sucesos.

Procesamiento de sucesos y mejora del servicio

Puede gestionar el procesamiento de sucesos, a través de la consola basada en web de Tivoli Netcool/Impact:

- Compruebe las conexiones de base de datos y de origen de datos.
- Compruebe que EventProcessor se esté ejecutando.
- Busque políticas existentes en el registro y actualice el nivel de registro.
- Actualice las políticas existentes o cree nuevas políticas.

Para obtener más información sobre el servicio proceso y mejora de sucesos, consulte el enlace al centro de información de Tivoli Netcool/Impact al final de la sección de servidor de sucesos.

Bus de mensajería

Los tres métodos principales para gestionar el servicio de bus de mensajería son:

- Línea de mandatos
- Explorador: una aplicación administrativa basada en Eclipse
- Kit de herramientas: una aplicación basada en Eclipse que permite la administración y el desarrollo de la aplicación.

Puede gestionar flujos de comunicación, definir pruebas, transformaciones, integraciones y registro, con la herramienta de desarrollo GUI.

El kit de herramientas de WebSphere Message Broker se proporciona con IBM Intelligent Operations Center. Para obtener más información sobre la instalación y el uso del kit de herramientas, consulte el enlace a WebSphere Message Broker Information Center al final de la sección servidor de sucesos

Para configurar el entorno de línea de mandatos y consultar instancias de WebSphere Message Broker:

- Inicie sesión en el servidor como usuario `mqm`.
- Vaya al directorio `/opt/IBM/mqsi/8.0.0.0`.
- Para configurar el entorno, ejecute el mandato `source bin/mqsiprofile`.
- Para consultar instancias de WebSphere Message Broker, ejecute el mandato: `bin/mqsilist`.

Para obtener más información sobre el servicio de mensaje de bus, consulte el enlace a WebSphere Message Broker Information Center al final de la sección de servidor de sucesos.

Servicio de administración de procedimiento operativo estándar

Puede definir los recursos y las actividades para gestionar sucesos a través de la consola de administración de procedimiento operativo estándar, centro de inicio de Tivoli Service Request Manager.

Para obtener más información sobre el servicio de administración de procedimiento operativo estándar, consulte el enlace de Tivoli Service Request Manager Information Center al final de la sección de servidor de sucesos.

Servicio de aplicaciones de procedimiento operativo estándar

Puede gestionar las aplicaciones asociadas con recursos o actividades mediante la consola basada en web de WebSphere Application Server, que sirve a Tivoli Service Request Manager.

Para obtener más información sobre el servicio de aplicaciones deprocedimiento operativo estándar, consulte la ayuda en línea o siga el enlace al Information Center deWebSphere Application Server Versión 7.0 que encontrará al final de la sección servidor de aplicaciones.

Conceptos relacionados:

"Configuración de Tivoli Service Request Manager" en la página 127
En la interfaz de usuario de Tivoli Service Request Manager , puede gestionar procedimientos de operación estándar, flujos de trabajo y recursos.

Información relacionada:

IBM Lotus Domino and Notes information center

IBM Tivoli Netcool/Impact information center

IBM WebSphere Message Broker information center

IBM Tivoli Service Request Manager information center

Servidor de gestión

Servicio de supervisión de aplicaciones

Puede gestionar la supervisión de aplicaciones a través de la consola basada en web de Tivoli Monitoring. Descargue la aplicación y ejecútela para comprobar el estado de los servidores y ver todos los agentes de supervisión que se están ejecutando. Para iniciar sesión, introduzca el ID de usuario y la contraseña. El ID de usuario predeterminado es sysadmin y la contraseña de topología es la introducida durante la instalación.

Para obtener más información sobre el servicio de supervisión de aplicaciones, consulte el enlace a la Guía del usuario de Tivoli Enterprise Portal al final del tema.

Servidor de aplicaciones para el servicio de gestión

Puede gestionar uniones de Tivoli Access Manager WebSEAL en la consola basada en web común, la consola Integrated Solutions.

Para obtener más información sobre este servicio, consulte la ayuda en línea o consulte el enlace de WebSphere Application Server Versión 7.0 Information Center al final de la sección de servidor de aplicaciones.

Servicio de base de datos

Existe una instancia de servicio de base de datos, `db2inst2`, alojada en el servidor de gestión. Puede utilizar esta instancia para la gestión de sistemas y el almacenamiento de datos específicos de Tivoli Access Manager.

Para obtener más información sobre el servicio de base de datos, consulte el enlace a IBM DB2 Database Information Center al final de la sección de servidor de datos.

Servicio de directorio

Gestione el directorio de usuarios a través de la consola basada en web de Tivoli Directory Server, podrá ver, añadir o cambiar usuarios en LDAP.

Para obtener más información sobre el servicio de directorio, consulte el enlace de Tivoli Directory Server Information Center, al final de este tema.

Información relacionada:

Guía del usuario de IBM Tivoli Monitoring, Tivoli Enterprise Portal

IBM Tivoli Directory Server information center

Verificación de componentes

La herramienta Comprobación de verificación del sistema prueba componentes dentro de IBM Intelligent Operations Center para determinar si son accesibles y operativos.

Cómo utilizar la herramienta Comprobación de verificación del sistema

La herramienta Comprobación de verificación del sistema se utiliza para determinar el estado operativo de los servicios que forman el sistemaIBM Intelligent Operations Center.

Acerca de esta tarea

La herramienta Comprobación de verificación del sistema verifica las prestaciones del sistema.

Para obtener detalles sobre las pruebas individuales y la resolución de problemas si las pruebas fracasan, pulse **Ayuda** para la prueba.

Propiedades proporciona información adicional sobre la prueba que debe utilizarse cuando se llama al soporte de software de IBM.

Procedimiento

1. Inicie sesión en IBM Intelligent Operations Center como un usuario con autorización de administrador.
2. Pulse **Intelligent Operations** > **Herramientas de administración** > **Comprobación de verificación del sistema**.
3. Seleccione la prueba o las pruebas que se van a ejecutar haciendo una de las siguientes cosas:
   - Pulse en una prueba específica para ejecutarla.
   - Pulse **Ejecutar todas las pruebas** para probar las prestaciones de todas las selecciones.

Resultados

El icono de  se muestra cuando una prueba se realiza correctamente. El icono de  se muestra cuando una prueba fracasa. Si una prueba fracasa, siga las instrucciones de determinación de problemas correspondientes a la prueba para resolver los errores. También se puede acceder a estas instrucciones haciendo clic en el icono de  o en **Ayuda** .

Si se ha ejecutado una prueba específica, los resultados de la ejecución de la prueba se visualizan en la parte inferior del portlet junto con el tiempo de ejecución de la prueba. Si se ha seleccionado **Ejecutar todas las pruebas**, esta información no se visualiza.

Qué hacer a continuación

La herramienta se puede restablecer, y borrarse todos los resultados, pulsando **Restablecer**.

Tareas relacionadas:

"Verificación de la instalación" en la página 52
Después de instalar IBM Intelligent Operations Center, verifique que el producto se ha instalado correctamente.

"Instalación de la herramienta Comprobación de verificación del sistema" en la página 50
La herramienta Comprobación de verificación del sistema se utiliza para verificar el estado operativo de los componentes en IBM Intelligent Operations Center. La herramienta se instalada independiente del producto.

Pruebas de Comprobación de verificación del sistema

IBM Intelligent Operations Center proporciona un número de pruebas de Comprobación de verificación del sistema que pueden utilizarse para determinar el estado operativo de varios servicios de IBM Intelligent Operations Center y componentes.

Las pruebas se agrupan de forma lógica según su función. Por la colaboración y supervisión.

Prueba de Gestión de cuentas (Tivoli Identity Manager API)

La prueba de Gestión de cuentas (Tivoli Identity Manager API) prueba el acceso a la API de Tivoli Identity Manager mediante el acceso al puerto de IIOP.

Recursos

La prueba de Gestión de cuentas (Tivoli Identity Manager API) utiliza los siguientes recursos:

- Tivoli Identity Manager Server (en servidor de gestión).

Determinación de problemas

Si falla la prueba de Gestión de cuentas (Tivoli Identity Manager API) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Compruebe que haya conectividad de red entre el servidor de aplicaciones y el servidor de gestión. Esto puede hacerse mediante el envío de mandatos de **ping** con el nombre de host abreviado y el completo de servidor de gestión desde el servidor de aplicaciones . Los resultados de los mandatos **ping** mostrarán si el DNS o el archivo `/etc/hosts` están resolviendo correctamente el nombre de host.
2. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de gestión revise los siguientes registros de Tivoli Identity Manager:
      - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log`
      - Todos los registros en los subdirectorios V6 del directorio `/var/idsldap/`.
3. Verifique que los sistemas de archivos de servidor de aplicaciones y servidor de gestión no han alcanzado su capacidad máxima. Esto puede determinarse mediante el mandato **df -h**.
4. Compruebe que el servidor de Tivoli Identity Manager se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos manuales:
   a. En el sistema de servidor de gestión, inicie sesión como `ibmadmin`.
   b. En una ventana de mandatos, ejecute: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/serverStatus.sh -all -username waswebadmin -password` *CONTRASEÑA_ADMIN_WAS* donde *CONTRASEÑA_ADMIN_WAS* es la contraseña de administrador de WebSphere Application Server.
   c. Si el mensaje `ADMU0509I: El servidor de aplicaciones "nodeagent" no es accesible. Parece estar detenido.` se visualiza, inicie el nodeagent utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "nodeagent" está STARTED.` . Si tuviera que iniciar el nodeagent, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor nodeagent abierto para e-business; el ID de proceso es 26654`.
   a. Si el mensaje `ADMU0509I: El servidor de aplicaciones "timServer1" no es accesible. Parece estar detenido.` se visualiza, inicie timServer1 utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startServer.sh timServer1`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "timServer1" está STARTED.` . Si tuviera que iniciar timServer1, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor timserver abierto para e-business; el ID de proceso es 26654`.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. timServer1

   Detenga los servidores en este orden:
   a. timServer1
   b. nodeagent

   El servidor timServer1 se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopServer.sh timServer1 -username waswebadmin -password` *CONTRAS_ADMIN_WAS* donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de gestión: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

5. Compruebe que el servidor de Tivoli Identity Manager se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos utilizando la WebSphere Application Server Administrative Console:
   a. Inicie sesión en la WebSphere Application Server Administrative Console en `http://`*`HOST_SERVIDOR_GESTIÓN`*`:9060/admin` utilizando el ID administrativo admin y la contraseña de WebSphere Application Server. *HOST_SERVIDOR_GESTIÓN* es el nombre de host para servidor de gestión.
   b. Vea el estado del servidor timServer1 pulsando **Servidores** > **Tipos de servidor** > **WebSphere Application Servers**.

      El icono de  significa que el servidor se ha iniciado. Si es necesario, seleccione el servidor y pulse **Reiniciar** para reiniciar el servidor.

      El icono de  significa que el servidor está detenido. Seleccione el servidor y haga clic en **Iniciar** para iniciar el servidor.

      El icono de  significa que el estado del servidor no está disponible. Puede que el agente del nodo no se esté ejecutando. Para iniciar el agente de nodo, ejecute el mandato `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh` en una ventana de mandatos.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. timServer1

   Detenga los servidores en este orden:
   a. timServer1
   b. nodeagent

   Para detener el servidor timServer1, seleccione el servidor y pulse **Detener**.

   El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de gestión: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.
6. Verifique que se puede acceder a la consola de Tivoli Identity Manager desde el sistema de WebSphere Portal, en servidor de aplicaciones, utilizando el siguiente URL: `http://`*`HOST_SERVIDOR_GESTIÓN`*`:9080/itim/console/main`. Donde *HOST_SERVIDOR_GESTIÓN* es el nombre de host para servidor de gestión. Inicie sesión con el ID de usuario `itim manager`.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Gestión de cuentas (Tivoli Identity Manager Console)

La prueba Gestión de cuentas (Tivoli Identity Manager Console) determina si se puede acceder a Tivoli Identity Manager por medio de la URL de Tivoli Identity Manager Administration.

Recursos

La prueba de Gestión de cuentas (Tivoli Identity Manager Console) utiliza los siguientes recursos:

- Tivoli Identity Manager Server (en servidor de gestión).

Determinación de problemas

Si falla la prueba de Gestión de cuentas (Tivoli Identity Manager Console) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Compruebe que haya conectividad de red entre el servidor de aplicaciones y el servidor de gestión. Esto puede hacerse mediante el envío de mandatos de **ping** con el nombre de host abreviado y el completo de servidor de gestión desde el servidor de aplicaciones . Los resultados de los mandatos **ping** mostrarán si el DNS o el archivo `/etc/hosts` están resolviendo correctamente el nombre de host.
2. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de gestión revise los siguientes registros de Tivoli Identity Manager:
      - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log`
      - Todos los registros en los subdirectorios V6 del directorio `/var/idsldap/`.
3. Verifique que los sistemas de archivos de servidor de aplicaciones y servidor de gestión no han alcanzado su capacidad máxima. Esto puede determinarse mediante el mandato **df -h**.
4. Compruebe que el servidor de Tivoli Identity Manager se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos manuales:
   a. En el sistema de servidor de gestión, inicie sesión como `ibmadmin`.
   b. En una ventana de mandatos, ejecute: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/serverStatus.sh -all -username waswebadmin -password` *CONTRASEÑA_ADMIN_WAS* donde *CONTRASEÑA_ADMIN_WAS* es la contraseña de administrador de WebSphere Application Server.
   c. Si el mensaje `ADMU0509I: El servidor de aplicaciones "nodeagent" no es accesible. Parece estar detenido.` se visualiza, inicie el nodeagent utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "nodeagent" está STARTED.` . Si tuviera que iniciar el nodeagent, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor nodeagent abierto para e-business; el ID de proceso es 26654`.
   a. Si el mensaje `ADMU0509I: El servidor de aplicaciones "timServer1" no es accesible. Parece estar detenido.` se visualiza, inicie timServer1 utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startServer.sh timServer1`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "timServer1" está STARTED.` . Si tuviera que iniciar timServer1, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor timserver abierto para e-business; el ID de proceso es 26654`.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:

   a. nodeagent
   b. timServer1

   Detenga los servidores en este orden:

a. timServer1
b. nodeagent

El servidor timServer1 se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopServer.sh timServer1 -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`* donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de gestión: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

5. Compruebe que el servidor de Tivoli Identity Manager se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos utilizando la WebSphere Application Server Administrative Console:
   a. Inicie sesión en la WebSphere Application Server Administrative Console en `http://`*`HOST_SERVIDOR_GESTIÓN`*`:9060/admin` utilizando el ID administrativo admin y la contraseña de WebSphere Application Server. *HOST_SERVIDOR_GESTIÓN* es el nombre de host para servidor de gestión.
   b. Vea el estado del servidor timServer1 pulsando **Servidores** > **Tipos de servidor** > **WebSphere Application Servers**.

      El icono de  significa que el servidor se ha iniciado. Si es necesario, seleccione el servidor y pulse **Reiniciar** para reiniciar el servidor.

      El icono de  significa que el servidor está detenido. Seleccione el servidor y haga clic en **Iniciar** para iniciar el servidor.

      El icono de  significa que el estado del servidor no está disponible. Puede que el agente del nodo no se esté ejecutando. Para iniciar el agente de nodo, ejecute el mandato `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh` en una ventana de mandatos.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. timServer1

   Detenga los servidores en este orden:
   a. timServer1
   b. nodeagent

   Para detener el servidor timServer1, seleccione el servidor y pulse **Detener**.

   El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de gestión: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.
6. Verifique que se puede acceder a la consola de Tivoli Identity Manager desde el sistema de WebSphere Portal, en servidor de aplicaciones, utilizando el siguiente URL: `http://`*`HOST_SERVIDOR_GESTIÓN`*`:9080/itim/console/main`. Donde *HOST_SERVIDOR_GESTIÓN* es el nombre de host para servidor de gestión. Inicie sesión con el ID de usuario `itim manager`.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Gestión de cuentas (conjunto de lista de Tivoli Directory Integrator)

La prueba de Gestión de cuentas (conjunto de lista de Tivoli Directory Integrator) determina si los recursos de Tivoli Directory Integrator List Assembly están disponibles. Para hacer esto, el mandato **tdisrvctl** , que gestiona configuraciones remotamente, ensambla líneas y otras funciones, se ejecuta en servidor de gestión y la prueba busca `"--- AssemblyLines ---"` para que sea devuelto.

Recursos

La prueba de Gestión de cuentas (conjunto de lista de Tivoli Directory Integrator) utiliza los siguientes recursos:

- Tivoli Directory Server (en servidor de datos)
- Tivoli Directory Integrator (en el servidor de gestión)

Determinación de problemas

Si falla la prueba de Gestión de cuentas (conjunto de lista de Tivoli Directory Integrator) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Compruebe que haya conectividad de red entre el servidor de aplicaciones y el servidor de datos. Esto puede hacerse mediante el envío de mandatos de **ping** con el nombre de host abreviado y el completo de servidor de datos desde el servidor de aplicaciones . Los resultados de los mandatos **ping** mostrarán si el DNS o el archivo `/etc/hosts` están resolviendo correctamente el nombre de host.
2. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verifique que los sistemas de archivo de los sistemas servidor de datos y servidor de aplicaciones no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **df -h**.
4. Verifique que Tivoli Directory Server se está ejecutando.
   a. Inicie sesión en una sesión de terminal en servidor de gestión as `ibmadmin`.
   b. Ejecute el mandato **ps -ef | grep ibmdisrv** . Los resultados serán similares a los siguientes:

      ```
      ibmadmin      11411       1  0 Sep06 pts/1    00:00:00 /bin/sh /opt/IBM/TDI/V7.1/ibmdisrv -s /opt/IBM/TDI/V7.1/timsol -c ITIM_RMI.xml -d
      ibmadmin      32080 19149  0 23:17 pts/1    00:00:00 grep ibmdisrv
      ```

      Este ejemplo muestra que el daemnon de Tivoli Directory Integrator Server, ibmdisrv, se está ejecutando.
5. Inicie el Tivoli Directory Integrator Server, ibmdisrv, si no se está ejecutando.
   a. Inicie sesión en una sesión de terminal en el servidor de gestión como `root`.
   b. Ejecute `/etc/init.d/ITIMAd start`.
6. Verifique que el servidor LDAP de Tivoli Directory Server se está ejecutando.
   a. Inicie sesión en una sesión de terminal en servidor de datos como `root`.
   b. Ejecute el mandato **ps -ef | grep ibmslapd**. Los resultados serán similares a los siguientes:

      ```
      dsrdbm01 13797     1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
      root     32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
      ```

      Este ejemplo muestra que el daemon de Tivoli Directory Server, ibmslapd, se está ejecutando.
   c. Ejecute el mandato **ps -ef | grep ibmdiradm**. Los resultados serán similares a los siguientes:

      ```
      root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
      dsrdbm01 11055     1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
      ```

      Este ejemplo muestra que el daemon de Tivoli Directory Server, ibmdiradm, se está ejecutando.
7. Si Tivoli Directory Server, ibmslapd, no se está ejecutando, realice lo siguiente.
   a. Como usuario *root* de Linux, ejecute **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** para iniciar Directory Server

8. Si Tivoli Directory Administration Server, ibmdiradm, no se está ejecutando, realice lo siguiente.
   a. En una sesión de terminal, en servidor de datos, ejecute **su - dsrdbm01**.
   b. Ejecute **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** para iniciar servidor de aplicaciones.
9. Si Tivoli Directory Server, ibmslapd, se está ejecutando, realice lo siguiente.

   Nota: Realice este paso incluso si Tivoli Directory Server se ha iniciado en el paso anterior.
   a. Inicie sesión en una sesión de terminal en servidor de datos como dsrdbm01.
   b. Ejecute **idsldapsearch -h localhost -D "cn=root" -w "***CONTRASEÑA_ADMIN***" -s sub uid=***, donde *CONTRASEÑA_ADMIN* es la contraseña de la cuenta de administrador de rol de LDAP. Se visualizarán los objetos de usuario LDAP existentes.
10. Verifique que la Tivoli Directory Server Web Administration Tool se está ejecutando. La Tivoli Directory Server Web Administration Tool se utiliza para detener e iniciar la instancia de LDAP, añadir usuarios o cuentas y ver archivos de registro.
    a. Inicie sesión en una sesión de terminal en servidor de gestión como ibmadmin.
    b. Ejecute el mandato **/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/serverStatus.sh -all -username waswebadmin -password** *CONTRASEÑA_ADMIN_WAS* en servidor de gestión donde *CONTRASEÑA_ADMIN_WAS* es la contraseña de administrador de WebSphere Application Server. Si la herramienta se está ejecutando, se devuelve un mensaje similar al siguiente.

       ```
       ADMU0508I: El servidor de aplicaciones "tdsServer" está STARTED
       ```

       Si se devuelve el siguiente mensaje, es necesario iniciar el tdsServer.

       ```
       ADMU0509I: No se puede alcanzar el servidor de aplicaciones "tdsServer". Parece que está parado.
       ```
    c. Inicie el tdsServer ejecutando el mandato **/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/startServer.sh tdsServer** . El servidor, tdsServer, se iniciará y se visualizará un mensaje similar al siguiente:

       ```
       ADMU3000I: Servidor tdsServer abierto para e-business; el ID de proceso es 26654.
       ```
11. Acceda a la Tivoli Directory Server Web Administration Tool en: http://*HOST_SERVIDOR_GESTIÓN*:9062/IDSWebApp/IDSjsp/Login.jsp donde *HOST_SERVIDOR_GESTIÓN* es el nombre de host de servidor de gestión.
12. Inicie sesión con la cuenta de administrador de rol LDAP, cn = root, y la contraseña apropiada. El nombre del servidor LDAP debe ser *HOST_SERVIDOR_DIRECTORIO_BASE_DATOS*:389 donde *HOST_SERVIDOR_DIRECTORIO_BASE_DATOS* es el nombre de host de servidor de datos.
13. Pulse **Administración de servidor** > **Iniciar/parar/restablecer servidor**. Se visualizará el estado del servidor LDAP. Esta página también se puede utilizar para iniciar, detener o restablecer el servidor LDAP.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Gestión de cuentas (Tivoli Directory Server)

La prueba de Gestión de cuentas (Tivoli Directory Server) determina si Tivoli Directory Server está disponible enviando una solicitud HTTP al servidor.

Recursos

La prueba de Gestión de cuentas (Tivoli Directory Server) utiliza los siguientes recursos:

- Tivoli Directory Server (en servidor de datos)

Determinación de problemas

Si **Tivoli Directory Server HTTP Test** falla, haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
2. Verifique que los sistemas de archivo de servidor de datos no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **df -h**.
3. Verifique que el servidor LDAP de Tivoli Directory Server se está ejecutando.
   a. Inicie sesión en una sesión de terminal en servidor de datos como `root`.
   b. Ejecute el mandato **ps -ef | grep ibmslapd**. Los resultados serán similares a los siguientes:

      ```
      dsrdbm01 13797     1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
      root     32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
      ```

      Este ejemplo muestra que el daemon de Tivoli Directory Server, ibmslapd, se está ejecutando.
   c. Ejecute el mandato **ps -ef | grep ibmdiradm**. Los resultados serán similares a los siguientes:

      ```
      root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
      dsrdbm01 11055     1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
      ```

      Este ejemplo muestra que el daemon de Tivoli Directory Server, ibmdiradm, se está ejecutando.
4. Si Tivoli Directory Server, ibmslapd, no se está ejecutando, realice lo siguiente.
   a. Como usuario *root* de Linux, ejecute **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** para iniciar Directory Server
5. Si Tivoli Directory Administration Server, ibmdiradm, no se está ejecutando, realice lo siguiente.
   a. En una sesión de terminal, en servidor de datos, ejecute **su - dsrdbm01**.
   b. Ejecute **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** para iniciar servidor de aplicaciones.
6. Si Tivoli Directory Server, ibmslapd, se está ejecutando, realice lo siguiente.

   Nota: Realice este paso incluso si Tivoli Directory Server se ha iniciado en el paso anterior.
   a. Inicie sesión en una sesión de terminal en servidor de datos como dsrdbm01.
   b. Ejecute **idsldapsearch -h localhost -D "cn=root" -w "***CONTRASEÑA_ADMIN***" -s sub uid=***, donde *CONTRASEÑA_ADMIN* es la contraseña de la cuenta de administrador de rol de LDAP. Se visualizarán los objetos de usuario LDAP existentes.
7. Verifique que la Tivoli Directory Server Web Administration Tool se está ejecutando. La Tivoli Directory Server Web Administration Tool se utiliza para detener e iniciar la instancia de LDAP, añadir usuarios o cuentas y ver archivos de registro.
   a. Inicie sesión en una sesión de terminal en servidor de gestión como `ibmadmin`.
   b. Ejecute el mandato **/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/serverStatus.sh -all -username waswebadmin -password** *CONTRASEÑA_ADMIN_WAS* en servidor de gestión donde *CONTRASEÑA_ADMIN_WAS* es la contraseña de administrador de WebSphere Application Server. Si la herramienta se está ejecutando, se devuelve un mensaje similar al siguiente.

      ```
      ADMU0508I: El servidor de aplicaciones "tdsServer" está STARTED
      ```

      Si se devuelve el siguiente mensaje, es necesario iniciar el tdsServer.

      ```
      ADMU0509I: No se puede alcanzar el servidor de aplicaciones "tdsServer". Parece que está parado.
      ```
   c. Inicie el tdsServer ejecutando el mandato **/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/startServer.sh tdsServer** . El servidor, tdsServer, se iniciará y se visualizará un mensaje similar al siguiente:

      ```
      ADMU3000I: Servidor tdsServer abierto para e-business; el ID de proceso es 26654.
      ```
8. Acceda a la Tivoli Directory Server Web Administration Tool en: `http://`*HOST_SERVIDOR_GESTIÓN*`:9062/IDSWebApp/IDSjsp/Login.jsp` donde *HOST_SERVIDOR_GESTIÓN* es el nombre de host de servidor de gestión.

9. Inicie sesión con la cuenta de administrador de rol LDAP, cn = root, y la contraseña apropiada. El nombre del servidor LDAP debe ser *HOST_SERVIDOR_DIRECTORIO_BASE_DATOS*:389 donde *HOST_SERVIDOR_DIRECTORIO_BASE_DATOS* es el nombre de host de servidor de datos.
10. Pulse **Administración de servidor** > **Iniciar/parar/restablecer servidor**. Se visualizará el estado del servidor LDAP. Esta página también se puede utilizar para iniciar, detener o restablecer el servidor LDAP.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Analítica (Cognos Gateway Console)

La prueba de Analítica (Cognos Gateway Console) determina si se puede acceder a Cognos, en el servidor de aplicaciones, mediante la Cognos Servlet Gateway y el URL de Cognos Administration Portal.

Recursos

La prueba de Analítica (Cognos Gateway Console) utiliza los siguientes recursos:

- Cognos (en el sistema servidor de aplicaciones).

Determinación de problemas

Si la prueba de Analítica (Cognos Gateway Console) no tiene éxito, realice lo siguiente para encontrar y resolver el problema de acceso.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de aplicaciones, revise los siguientes registros de Cognos:
      - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Disp1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Disp1/SystemErr.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemErr.log`
      - Todos los registros en el directorio `/opt/IBM/cognos/c10_64/logs/`.
2. Verifique que los sistemas de archivo del sistema servidor de aplicaciones no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **df -h**.
3. Verifique que los servidores Cognos Dispatcher y Cognos Gateway se han iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos manuales:
   a. En el sistema servidor de aplicaciones , inicie sesión como `cgnsadm` (usuario Cognos).
   b. En una ventana de mandato, ejecute: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *CONTRAS_ADMIN_WAS*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere Application Server.
   c. Si el mensaje `ADMU0509I: El servidor de aplicaciones "nodeagent" no es accesible. Parece estar detenido.` se visualiza, inicie el nodeagent utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startNode.sh`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "nodeagent" está STARTED.` . Si tuviera que iniciar el nodeagent, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor nodeagent abierto para e-business; el ID de proceso es 26654`.
   d. Si aparece el mensaje `ADMU0509I: No se puede alcanzar el "CognosX_Disp1" del servidor de aplicaciones. Parece estar detenido.` se visualiza, inicie CognosX_Disp1 utilizando el siguiente

mandato: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startServer.sh CognosX_Disp1`. Sáltese este paso si aparece el mensaje `ADMU0508I: el "CognosX_Disp1" del servidor de aplicaciones está INICIADO.` se muestra. Si tuviera que iniciar CognosX_Disp1, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor CognosX_Disp1 abierto para e-business; el ID de proceso es 26654`.

e. Si el mensaje `ADMU0509I: El servidor de aplicaciones "CognosX_GW1" no es accesible. Parece estar detenido.` Si se muestra, inicie CognosX_GW1 utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startServer.sh CognosX_GW1`. Sáltese este paso si aparece el mensaje `ADMU0508I: el "CognosX_GW1" del servidor de aplicaciones está INICIADO.` se muestra. Si tuviera que iniciar CognosX_GW1, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor CognosX_GW1 abierto para e-business; el ID de proceso es 26676`.

Importante: Los servidores deben iniciarse y detenerse en un orden específico.

Inicie los servidores en este orden:

a. nodeagent
b. CognosX_Disp1
c. CognosX_GW1

Detenga los servidores en este orden:

a. CognosX_GW1
b. CognosX_Disp1
c. nodeagent

El servidor CognosX_GW1 se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopServer.sh CognosX_GW1 -username waswebadmin -password` *`CONTR_ADMIN_WAS`*, donde *CONTR_ADMIN_WAS* es la contraseña del administrador de WebSphere.

El servidor CognosX_Disp1 se detiene ejecutando el siguiente mandato en una ventana de mandato del servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopServer.sh CognosX_GW1 -username waswebadmin -password` *`CONTR_ADMIN_WAS`*, donde *CONTR_ADMIN_WAS* es la contraseña del administrador de WebSphere.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTR_ADMIN_WAS`*, donde *CONTR_ADMIN_WAS* es la contraseña del administrador de WebSphere.

4. Verifique que los servidores Cognos Dispatcher y Cognos Gateway se han iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos utilizando la WebSphere Application Server Administrative Console:
   a. Inicie sesión en la WebSphere Application Server Administrative Console en `http://` *`HOST_SERVIDOR_APLICACIONES`*`:9060/admin` utilizando el ID administrativo admin y la contraseña de WebSphere Application Server. *HOST_SERVIDOR_APLICACIONES* es el nombre de host para servidor de aplicaciones.
   b. Vea el estado de los servidores CognosX-Disp1 y CognosX_GW1, pulsando **Servidores** > **Tipos de servidor** > **Servidores de aplicación WebSphere**.

      El icono de  significa que el servidor se ha iniciado. Si es necesario, seleccione el servidor y pulse **Reiniciar** para reiniciar el servidor.

      El icono de  significa que el servidor está detenido. Seleccione el servidor y haga clic en **Iniciar** para iniciar el servidor.

El icono de ? significa que el estado del servidor no está disponible. Puede que el agente del nodo no se esté ejecutando. Para iniciar el agente de nodo, ejecute el mandato `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startNode.sh` en una ventana de mandatos.

Importante: Los servidores deben iniciarse y detenerse en un orden específico.

Inicie los servidores en este orden:

a. nodeagent
b. CognosX_Disp1
c. CognosX_GW1

Detenga los servidores en este orden:

a. CognosX_GW1
b. CognosX_Disp1
c. nodeagent

Para detener los servidores CognosX_GW1 y CognosX_Disp1, seleccione el servidor y pulse **Detener**.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTR_ADMIN_WAS`*, donde *CONTR_ADMIN_WAS* es la contraseña del administrador de WebSphere.

5. Verifique que se puede acceder al portal de administración Cognos desde el sistema de portal WebSphere , en servidor de aplicaciones, utilizando la siguiente URL: `http://` *`APPLICATION_SERVER_HOST`*`:9081/ServletGateway/servlet/Gateway`. Donde *HOST_SERVIDOR_APLICACIONES* es el nombre de host para el servidor de aplicaciones.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Servidor de aplicaciones (WebSphere Application Server Web Service)

La prueba de Servidor de aplicaciones (WebSphere Application Server Web Service) prueba el acceso al WebSphere Application Server Web Service mediante el acceso al servicio web DrpGeoSvcs.

Recursos

La prueba de Servidor de aplicaciones (WebSphere Application Server Web Service) utiliza los siguientes recursos:

- WebSphere Application Server (en servidor de aplicaciones).

Determinación de problemas

Si falla la prueba de Servidor de aplicaciones (WebSphere Application Server Web Service) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de aplicaciones, revise los siguientes registros de configuración de WebSphere UDDI Registry:
      - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log`

- /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log

2. Verifique que el sistema de archivos de servidor de aplicaciones no ha alcanzado su capacidad máxima. Esto puede determinarse mediante el mandato **df -h**.
3. Verifique que el servidor cpudServer1 se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos manuales:
   a. En el sistema de servidor de aplicaciones, inicie sesión como ibmadmin.
   b. En una ventana de mandato, ejecute: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/serverStatus.sh -all -username waswebadmin -password *CONTRAS_ADMIN_WAS*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere Application Server.
   c. Si el mensaje ADMU0509I: El servidor de aplicaciones "nodeagent" no es accesible. Parece estar detenido. se visualiza, inicie el nodeagent utilizando el siguiente mandato: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh. Omita este paso si se visualiza el mensaje ADMU0508I: El servidor de aplicaciones "nodeagent" está STARTED. . Si tuviera que iniciar el nodeagent, se visualizará un mensaje similar al siguiente: ADMU3000I: Servidor nodeagent abierto para e-business; el ID de proceso es 26654.
   a. Si el mensaje ADMU0509I: El servidor de aplicaciones "cpudServer1" no es accesible. Parece estar detenido. se visualiza, inicie el cpdudServer1 utilizando el siguiente mandato: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startServer.sh cpudServer1. Omita este paso si se visualiza el mensaje ADMU0508I: El servidor de aplicaciones "cpudServer1" está STARTED. . Si tuviera que iniciar cpudServer1, se visualizará un mensaje similar al siguiente: ADMU3000I: Servidor cpudServer1 abierto para e-business; el ID de proceso es 26654.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. cpudServer1

   Detenga los servidores en este orden:
   a. cpudServer1
   b. nodeagent

   El servidor cpudServer1 se detiene ejecutando el siguiente mandato en una ventana de mandatos de servidor de aplicaciones: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password *WAS_ADMIN_PWD* donde *WAS_ADMIN_PWD* es la contraseña de administrador de WebSphere.

   El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password *CONTRAS_ADMIN_WAS*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.
4. Verifique que el servidor cpudServer1 se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos utilizando la WebSphere Application Server Administrative Console:
   a. Inicie sesión en la WebSphere Application Server Administrative Console en http://*HOST_SERVIDOR_APLICACIONES*:9060/admin utilizando el ID administrativo admin y la contraseña de WebSphere Application Server. *HOST_SERVIDOR_APLICACIONES* es el nombre de host para el servidor de aplicaciones.
   b. Vea el estado del servidor cpudServer1 pulsando **Servidores** > **Tipos de servidor** > **WebSphere Application Servers**.

      El icono de  significa que el servidor se ha iniciado. Si es necesario, seleccione el servidor y pulse **Reiniciar** para reiniciar el servidor.

El icono de significa que el servidor está detenido. Seleccione el servidor y haga clic en **Iniciar** para iniciar el servidor.

El icono de significa que el estado del servidor no está disponible. Puede que el agente del nodo no se esté ejecutando. Para iniciar el agente de nodo, ejecute el mandato `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh` en una ventana de mandatos.

Importante: Los servidores deben iniciarse y detenerse en un orden específico.

Inicie los servidores en este orden:

a. nodeagent
b. cpudServer1

Detenga los servidores en este orden:

a. cpudServer1
b. nodeagent

Para detener el servidor cpudServer, seleccione el servidor y pulse **Detener**.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

5. Verifique que se puede acceder a la WebSphere UDDI User Console.
   a. En servidor de aplicaciones, acceda a: `https://`*`HOST_SERVIDOR_APLICACIONES`*`:9080/uddigui/`, donde *HOST_SERVIDOR_APLICACIONES* es el nombre de host de servidor de aplicaciones.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Reglas de negocio (WebSphere Operational Decision Manager JRules Console)

La prueba Reglas de negocio (WebSphere Operational Decision Manager JRules Console) prueba el acceso a WebSphere Operational Decision Management JRules accediendo a la consola Rule Execution Server.

Recursos

La prueba de Reglas de negocio (WebSphere Operational Decision Manager JRules Console) utiliza los siguientes recursos:

- WebSphere Operational Decision Management JRules (en servidor de aplicaciones).

Determinación de problemas

Si falla la prueba de Reglas de negocio (WebSphere Operational Decision Manager JRules Console) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de aplicaciones revise los siguientes registros de configuración de WebSphere Operational Decision Management:
      - `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log`

- /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log

2. Verifique que el sistema de archivos de servidor de aplicaciones no ha alcanzado su capacidad máxima. Esto puede determinarse mediante el mandato **df -h**.
3. Verifique que el Rule Execution Server se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos manuales:
   a. En el sistema de servidor de aplicaciones, inicie sesión como ibmadmin.
   b. En una ventana de mandato, ejecute: /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/serverStatus.sh -all -username waswebadmin -password *CONTRAS_ADMIN_WAS*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere Application Server.
   c. Si el mensaje ADMU0509I: El servidor de aplicaciones "nodeagent" no es accesible. Parece estar detenido. se visualiza, inicie el nodeagent utilizando el siguiente mandato: /opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh. Omita este paso si se visualiza el mensaje ADMU0508I: El servidor de aplicaciones "nodeagent" está STARTED. . Si tuviera que iniciar el nodeagent, se visualizará un mensaje similar al siguiente: ADMU3000I: Servidor nodeagent abierto para e-business; el ID de proceso es 26654.
   a. Si el mensaje ADMU0509I: El servidor de aplicaciones "wodmServer1" no es accesible. Parece estar detenido. se visualiza, inicie wodmServer1 utilizando el siguiente mandato: /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/startServer.sh wodmServer1. Omita este paso si se visualiza el mensaje ADMU0508I: El servidor de aplicaciones "wodmServer1" está STARTED. . Si tuviera que iniciar wodmServer1, se visualizará un mensaje similar al siguiente: ADMU3000I: Servidor wodmServer1 abierto para e-business; el ID de proceso es 26654.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. wodmServer1

   Detenga los servidores en este orden:
   a. wodmServer1
   b. nodeagent

   El servidor wodmServer1 se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopServer.sh wodmServer1 -username waswebadmin -password *CONTRAS_ADMIN_WAS* donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

   El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password *CONTRAS_ADMIN_WAS*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.
4. Verifique que el Rule Execution Server se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos utilizando la WebSphere Application Server Administrative Console:
   a. Inicie sesión en la WebSphere Application Server Administrative Console en http://*HOST_SERVIDOR_APLICACIONES*:9060/admin utilizando el ID administrativo admin y la contraseña de WebSphere Application Server. *HOST_SERVIDOR_APLICACIONES* es el nombre de host para servidor de aplicaciones.
   b. Vea el estado del servidor wodmProfile pulsando **Servidores** > **Tipos de servidor** > **WebSphere Application Servers**.

      El icono de  significa que el servidor se ha iniciado. Si es necesario, seleccione el servidor y pulse **Reiniciar** para reiniciar el servidor.

El icono de  significa que el servidor está detenido. Seleccione el servidor y haga clic en **Iniciar** para iniciar el servidor.

El icono de  significa que el estado del servidor no está disponible. Puede que el agente del nodo no se esté ejecutando. Para iniciar el agente de nodo, ejecute el mandato `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` en una ventana de mandatos.

Importante: Los servidores deben iniciarse y detenerse en un orden específico.

Inicie los servidores en este orden:

a. nodeagent
b. wodmServer1

Detenga los servidores en este orden:

a. wodmServer1
b. nodeagent

Para detener el servidor wodmProfile, seleccione el servidor y pulse **Detener**.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

5. Verifique que se puede acceder a la Rule Execution Server Console desde servidor de aplicaciones en `http://`*`HOST_SERVIDOR_APLICACIONES`*`:9083/res`, donde *HOST_SERVIDOR_APLICACIONES* es el nombre de host de servidor de aplicaciones. Inicie sesión utilizando el ID de usuario `resAdmin1`.
6. En la Rule Execution Server Console, abra el separador Diagnóstico. Pulse **Ejecutar diagnósticos**. Se visualizará un informe con la ejecución de prueba. Pulse **Expandir todo** para ver los detalles sobre cada prueba.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Reglas de negocio (WebSphere Operational Decision Manager JRules Rule)

Las pruebas de Reglas de negocio (WebSphere Operational Decision Manager JRules Rule) acceden al WebSphere Operational Decision Management JRules Rule Engine mediante una llamada a la regla de negocio `cardTransactionRuleApp` instalada en el Rule Execution Server y la verificación de la salida.

Recursos

La prueba de Reglas de negocio (WebSphere Operational Decision Manager JRules Rule) utiliza los siguientes recursos:

- WebSphere Operational Decision Management JRules (en servidor de aplicaciones).

Determinación de problemas

Si falla la prueba de Reglas de negocio (WebSphere Operational Decision Manager JRules Rule) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`

- /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log

b. En servidor de aplicaciones revise los siguientes registros de configuración de WebSphere Operational Decision Management:
   - /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log
   - /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log

2. Verifique que el sistema de archivos de servidor de aplicaciones no ha alcanzado su capacidad máxima. Esto puede determinarse mediante el mandato **df -h**.
3. Verifique que el Rule Execution Server se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos manuales:
   a. En el sistema de servidor de aplicaciones, inicie sesión como ibmadmin.
   b. En una ventana de mandato, ejecute: /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/serverStatus.sh -all -username waswebadmin -password *CONTRAS_ADMIN_WAS*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere Application Server.
   c. Si el mensaje ADMU0509I: El servidor de aplicaciones "nodeagent" no es accesible. Parece estar detenido. se visualiza, inicie el nodeagent utilizando el siguiente mandato: /opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh. Omita este paso si se visualiza el mensaje ADMU0508I: El servidor de aplicaciones "nodeagent" está STARTED. . Si tuviera que iniciar el nodeagent, se visualizará un mensaje similar al siguiente: ADMU3000I: Servidor nodeagent abierto para e-business; el ID de proceso es 26654.
   a. Si el mensaje ADMU0509I: El servidor de aplicaciones "wodmServer1" no es accesible. Parece estar detenido. se visualiza, inicie wodmServer1 utilizando el siguiente mandato: /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/startServer.sh wodmServer1. Omita este paso si se visualiza el mensaje ADMU0508I: El servidor de aplicaciones "wodmServer1" está STARTED. . Si tuviera que iniciar wodmServer1, se visualizará un mensaje similar al siguiente: ADMU3000I: Servidor wodmServer1 abierto para e-business; el ID de proceso es 26654.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. wodmServer1

   Detenga los servidores en este orden:
   a. wodmServer1
   b. nodeagent

   El servidor wodmServer1 se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopServer.sh wodmServer1 -username waswebadmin -password *CONTRAS_ADMIN_WAS* donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

   El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password *CONTRAS_ADMIN_WAS*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.
4. Verifique que el Rule Execution Server se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos utilizando la WebSphere Application Server Administrative Console:
   a. Inicie sesión en la WebSphere Application Server Administrative Console en http://*HOST_SERVIDOR_APLICACIONES*:9060/admin utilizando el ID administrativo admin y la contraseña de WebSphere Application Server. *HOST_SERVIDOR_APLICACIONES* es el nombre de host para servidor de aplicaciones.

b. Vea el estado del servidor wodmProfile pulsando **Servidores** > **Tipos de servidor** > **WebSphere Application Servers**.

El icono de  significa que el servidor se ha iniciado. Si es necesario, seleccione el servidor y pulse **Reiniciar** para reiniciar el servidor.

El icono de  significa que el servidor está detenido. Seleccione el servidor y haga clic en **Iniciar** para iniciar el servidor.

El icono de  significa que el estado del servidor no está disponible. Puede que el agente del nodo no se esté ejecutando. Para iniciar el agente de nodo, ejecute el mandato `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` en una ventana de mandatos.

Importante: Los servidores deben iniciarse y detenerse en un orden específico.

Inicie los servidores en este orden:

a. nodeagent
b. wodmServer1

Detenga los servidores en este orden:

a. wodmServer1
b. nodeagent

Para detener el servidor wodmProfile, seleccione el servidor y pulse **Detener**.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

5. Verifique que se puede acceder a la Rule Execution Server Console desde servidor de aplicaciones en `http://`*`HOST_SERVIDOR_APLICACIONES`*`:9083/res`, donde *HOST_SERVIDOR_APLICACIONES* es el nombre de host de servidor de aplicaciones. Inicie sesión utilizando el ID de usuario `resAdmin1`.
6. En la Rule Execution Server Console, abra el separador Diagnóstico. Pulse **Ejecutar diagnósticos**. Se visualizará un informe con la ejecución de prueba. Pulse **Expandir todo** para ver los detalles sobre cada prueba.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Colaboración (Lotus Domino Console)

La prueba de Colaboración (Lotus Domino Console) determina si se puede acceder al directorio de Domino a través de su URL.

Recursos

La prueba de Colaboración (Lotus Domino Console) utiliza los siguientes recursos:

- Domino Server (en el servidor de sucesos).

Determinación de problemas

Si falla la prueba de Colaboración (Lotus Domino Console) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de sucesos, revise los siguientes registros de Lotus Domino:

- /local/notesdata/console.out
- /local/notesdata/log.nsf
- Todos los registros en el directorio /local/notesdata/IBM_TECHNICAL_SUPPORT/.

2. Verifique que los sistemas de archivo del sistema servidor de sucesos no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **df -h**.
3. Verifique que los componentes del proceso de Lotus Domino se están ejecutando.
   a. Inicie sesión en la consola del directorio de Lotus Domino en http://*EVENT_SERVER_HOST*:84/names.nsf donde *EVENT_SERVER_HOST* es el nombre de host deservidor de sucesos. Inicie sesión utilizando el nombre de usuario del administrador Domino y la contraseña.
   b. Si no se puede acceder a la consola, en el servidor de sucesos, ejecute el mandato ps -ef | grep notes para determinar si los procesos de Lotus Domino se están ejecutando. Los procesos de Lotus Domino son:
      - servidor
      - suceso
      - actualizar
      - replica
      - router
      - adminp
      - calconn
      - sched
      - http
      - rnrmgr
      - staddin
4. Si alguno, pero no todos los procesos se están ejecutando, detenga los procesos que se están ejecutando antes de reiniciar todos los procesos.
   a. En el servidor de sucesos, inicie sesión como el usuario notes.
   b. Cambie al directorio /local/notesdata.
   c. Ejecute el mandato "nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &" para detener todos los procesos de Lotus Domino en ejecución.
   d. Compruebe que se han detenido todos los procesos ejecutando el mandato ps -ef | grep notes .
   e. Si hay procesos de Lotus Domino que todavía se están ejecutando, deténgalos utilizando **kill -9** *pid* donde *pid* es el identificador de proceso del proceso Lotus Domino .
5. Si los procesos de Lotus Domino no se están ejecutando, inicie los componentes de Lotus Domino Server.
   a. En el servidor de sucesos, inicie sesión como el usuario notes.
   b. Cambie al directorio /local/notesdata.
   c. Ejecute el mandato "nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &" para iniciar todos los componentes de Lotus Domino Server.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Collaboration (Lotus Sametime Console)

La prueba de Collaboration (Lotus Sametime Console) determina si la Sametime Console es accesible a través de su URL.

Recursos

La prueba de Collaboration (Lotus Sametime Console) utiliza los siguientes recursos:

- Sametime Server (en servidor de sucesos).

Determinación de problemas

Si falla la prueba de Collaboration (Lotus Sametime Console) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Recopile y revise los archivos de configuración y registro del Sametime Community Server.
   a. Inicie sesión en el servidor de sucesos como un usuario *notes*.
   b. Cambie al directorio `/local/notesdata`.
   c. Ejecute el mandato `sh stdiagzip.sh` . Este mandato recopilará todos los archivos de registro pertinentes y los grabará al directorio`/local/notesdata/` .
   d. Revise los registros en el directorio `/local/notesdata/` .
2. Verifique que los sistemas de archivo del sistema servidor de sucesos no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **`df -h`**.
3. Verifique que los componentes de Sametime Process se están ejecutando.
   a. Inicie sesión en la página principal de Sametime en `http://`*`EVENT_SERVER_HOST`*`:84/stcenter.nsf` donde *EVENT_SERVER_HOST* es el nombre de host de servidor de sucesos. Inicie sesión utilizando el nombre de usuario del administrador Domino y la contraseña.
   b. En la página principal de Sametime pulse **Administrar el servidor**.
   c. En la página Servidor - Visión general, asegúrese de que todos los servicios de Sametime se están ejecutando.
4. Si alguno, pero no todos los procesos se están ejecutando, detenga los procesos que se están ejecutando antes de reiniciar todos los procesos.
   a. En el servidor de sucesos, inicie sesión como el usuario `notes`.
   b. Cambie al directorio `/local/notesdata`.
   c. Ejecute el mandato `"nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &"` para detener todos los procesos de Sametime que se están ejecutando.
   d. Compruebe que se han detenido todos los procesos ejecutando el mandato `ps -ef | grep notes` .
   e. Si todavía hay procesos que se están ejecutando, deténgalos utilizando **`kill -9`** *pid* donde *pid* es el identificador de proceso del proceso Lotus Domino .
5. Si no se están ejecutando procesos Sametime , inicie los componentes del servidorLotus Sametime .
   a. En el servidor de sucesos, inicie sesión como el usuario `notes`.
   b. Cambie al directorio `/local/notesdata`.
   c. Ejecute el mandato `"nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &"` para iniciar todos los componentes de Lotus Sametime Server.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Colaboración (Lotus Sametime Proxy)

La prueba de Colaboración (Lotus Sametime Proxy) determina si se puede acceder a Lotus Sametime Proxy Web Application mediante el URL de Lotus Sametime Proxy Web Application.

Recursos

La prueba de Colaboración (Lotus Sametime Proxy) utiliza los siguientes recursos:

- Sametime Proxy (en el servidor de aplicaciones).

Determinación de problemas

Si la prueba de Colaboración (Lotus Sametime Proxy) no tiene éxito, realice lo siguiente para encontrar y resolver el problema de acceso.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de aplicaciones, revise los siguientes registros de Sametime Proxy Server:
      - `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log`
2. Verifique que los sistemas de archivo del sistema servidor de aplicaciones no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **`df -h`**.
3. Verifique que Sametime Proxy Server se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos manuales:
   a. En el sistema de servidor de aplicaciones, inicie sesión como `ibmadmin`.
   b. En una ventana de mandatos, ejecute: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *`WAS_ADMIN_PWD`* donde *WAS_ADMIN_PWD* es la contraseña de administrador de WebSphere Application Server.
   c. Si el mensaje `ADMU0509I: El servidor de aplicaciones "nodeagent" no es accesible. Parece estar detenido.` se visualiza, inicie el nodeagent utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh` . Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "nodeagent" está STARTED.` . Si tuviera que iniciar el nodeagent, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor nodeagent abierto para e-business; el ID de proceso es 26654`.
   d. Si el mensaje `ADMU0509I: El servidor de aplicaciones "STProxyServer1" no es accesible. Parece estar detenido.` se visualiza, inicie STProxyServer1 utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/startServer.sh STProxyServer1`. Sáltese este paso si aparece el mensaje `ADMU0508I: el "STProxyServer1" del servidor de aplicaciones está INICIADO.` se muestra. Si tuviera que iniciar STProxyServer1, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor STProxyServer1 abierto para e-business; el ID de proceso es 26654`.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. STProxyServer1

   Detenga los servidores en este orden:
   a. STProxyServer1
   b. nodeagent

El servidor STProxyServer1 se detiene ejecutando el siguiente mandato en una ventana de mandato de Application Server: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopServer.sh STProxyServer1 -username waswebadmin -password` *`CONTR_ADMIN_WAS`*, donde *CONTR_ADMIN_WAS* es la contraseña del administrador de WebSphere.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de Application Server: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTR_ADMIN_WAS`*, donde *CONTR_ADMIN_WAS* es la contraseña del administrador de WebSphere.

4. Verifique que se ha iniciado el servidor proxy de Sametime . La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos utilizando la WebSphere Application Server Administrative Console:
   a. Inicie sesión en la WebSphere Application Server Administrative Console en `http://` *`APPLICATION_SERVER_HOST`*`:9060/admin` utilizando el ID de administrador y la contraseña de WebSphere Application Server Administrative. *HOST_SERVIDOR_APLICACIONES* es el nombre de host para servidor de aplicaciones.
   b. Vea el estado del servidor STProxyServer1 haciendo clic en **Servidores** > **Tipos de servidor** > **WebSphere Application Servers**.

      El icono de  significa que el servidor se ha iniciado. Si es necesario, seleccione el servidor y pulse **Reiniciar** para reiniciar el servidor.

      El icono de  significa que el servidor está detenido. Seleccione el servidor y haga clic en **Iniciar** para iniciar el servidor.

      El icono de  significa que el estado del servidor no está disponible. Puede que el agente del nodo no se esté ejecutando. Para iniciar el agente de nodo, ejecute el mandato `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh` en una ventana de mandatos.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. STProxyServer1

   Detenga los servidores en este orden:
   a. STProxyServer1
   b. nodeagent

   Para detener el servidor STProxyServer1, seleccione el servidor y haga clic en **Detener**.

   El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de Application Server: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTR_ADMIN_WAS`*, donde *CONTR_ADMIN_WAS* es la contraseña del administrador de WebSphere.
5. Verifique que se puede acceder a Sametime Proxy Console desde el sistema de WebSphere Portal, en servidor de aplicaciones, utilizando el siguiente URL: `http://`*`HOST_SERVIDOR_APLICACIONES`*`:9085/stwebclient/popup`. Donde *HOST_SERVIDOR_APLICACIONES* es el nombre de host para el servidor de aplicaciones.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Base de datos (DB2)

La prueba de Base de datos (DB2) determina si se puede acceder a la conexión JDBC entre la aplicación web y servidor de datos. Se establece una conexión JDBC tipo 4 y se emite una consulta SQL dinámica contando el número de tablas presentes en la base de datos.

Recursos

La prueba de Base de datos (DB2) utiliza los siguientes recursos:

- La definición `UddiDataSource` que contiene la conexión para la base de datos UDDIDB (en servidor de aplicaciones).
- Base de datos UDDIDB (instancia db2inst4 en servidor de datos).

Determinación de problemas

Si la prueba de Base de datos (DB2) no puede acceder al servidor de datos, realice lo siguiente para encontrar y resolver el problema de acceso.

Procedimiento

1. Compruebe que hay conectividad de red entre servidor de aplicaciones donde se inició la prueba y servidor de datos donde reside la base de datos. Esto puede hacerse mediante el envío de mandatos de **`ping`** con el nombre de host abreviado y el completo de servidor de datos desde el servidor de aplicaciones . Los resultados de los mandatos **`ping`** mostrarán si el DNS o el archivo `/etc/hosts` están resolviendo correctamente el nombre de host.
2. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verifique que los sistemas de archivo del sistema servidor de datos no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **`df -h`**.
4. Verifique que las bases de datos utilizadas por servidor de datos se han iniciado.
   a. En el servidor de datos, ejecute el siguiente mandato desde una ventana de mandato como db2inst4:

      ```
      ps -ef | grep db2 | grep db2inst4
      ```

      Los procesos de DB2 , incluyendo el siguiente, deben ejecutarse como usuario de instancia db2inst4:

      db2sysc

      db2vend

      db2acd
5. Si los procesos de DB2 no se están ejecutando, inícielos ejecutando `db2start` desde la ventana de mandatos como usuario db2inst4:
6. Compruebe los registros de DB2 para obtener errores relacionados con la instancia de base de datos utilizada para esta prueba. Los registros están ubicados en servidor de datos en el directorio`/datahome/db2inst4/sqllib/db2dump` .
7. Compruebe el archivo `db2diag.log` por si hay errores emitidos al iniciar la base de datos utilizada para esta prueba.
8. Verifique la conexión con los recursos del contenedor web DataSource mediante la consola de administración de WebSphere Application Server.
   a. En el servidor de aplicaciones, acceda a la consola de administración de WebSphere Application Server en: `https://`*`HOST_SERVIDOR_APLICACIONES`*`:9043/ibm/console`, donde *HOST_SERVIDOR_APLICACIONES* es el nombre de host del servidor de aplicaciones.
   b. Haga clic en **Recursos** > **JDBC** > **Orígenes de datos**.

c. Compruebe el origen de datos UddiDataSource pulsando **Probar conexión** para probar la conexión al origen de datos.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Base de datos (DB2 Instance - *instancia*)

Base de datos (DB2 Instance - *instancia*) prueba el estado del gestor de DB2 de la instancia de DB2 en el servidor de datos mediante la ejecución del script **db2status**.

Recursos

La prueba de Base de datos (DB2 Instance - *instancia*) utiliza los siguientes recursos:

- La instancia DB2 (en servidor de datos)

Determinación de problemas

Si la prueba de Base de datos (DB2 Instance - *instancia*) no tiene éxito, realice lo siguiente para encontrar y resolver el problema de acceso.

Procedimiento

1. Compruebe que hay conectividad de red entre servidor de aplicaciones donde se inició la prueba y servidor de datos donde reside la base de datos. Esto puede hacerse mediante el envío de mandatos de **ping** con el nombre de host abreviado y el completo de servidor de datos desde el servidor de aplicaciones . Los resultados de los mandatos **ping** mostrarán si el DNS o el archivo `/etc/hosts` están resolviendo correctamente el nombre de host.
2. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verifique que el sistema de archivos de servidor de datos no ha alcanzado su capacidad máxima. Esto puede determinarse mediante el mandato **df -h**.
4. Verifique que las bases de datos utilizadas por servidor de datos se han iniciado.
   a. En el servidor de datos, ejecute el siguiente mandato desde una ventana de mandato como el usuario *instancia*, donde *instancia* es el nombre de la instancia de DB2 indicada en el nombre de la prueba:

      ```
      db2 get snapshot for dbm | grep status
      ```

      Si se inicia el gestor de base de datos para la *instance*, se muestra el siguiente mensaje: `Database manager status = Active`.
5. Si los procesos de DB2 no se están ejecutando, inícielos ejecutando el mandato **su -** *instancia* desde la ventana de mandato si está ejecutando como el usuario `root`. De lo contrario, ejecute **db2start** para iniciar el gestor de bases de datos.
6. Compruebe los registros de DB2 para obtener errores relacionados con la instancia de base de datos utilizada para esta prueba. Los registros se encuentran en servidor de datos, en el directorio `/datahome/`*instancia*`/sqllib/db2dump`.
7. Compruebe el archivo `db2diag.log` por si hay errores emitidos al iniciar la base de datos utilizada para esta prueba.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Directorio (UDDI V3 and UDDI V3 HTTPS)

La prueba Directorio (UDDI V3 and UDDI V3 HTTPS) determina si se puede acceder al registro UDDI de WebSphere utilizando la URL de HTTP y HTTPS del registro UDDI de WebSphere .

Recursos

La prueba de Directorio (UDDI V3 and UDDI V3 HTTPS) utiliza los siguientes recursos:

- WebSphere Application Server (en servidor de aplicaciones).

Determinación de problemas

Si la prueba de Directorio (UDDI V3 and UDDI V3 HTTPS) no tiene éxito, realice lo siguiente para encontrar y resolver el problema de acceso.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de aplicaciones, revise los siguientes registros de configuración de WebSphere UDDI Registry:
      - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log`
2. Verifique que los sistemas de archivo del sistema servidor de aplicaciones no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **`df -h`**.
3. Verifique que el servidor cpudServer1 se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos manuales:
   a. En el sistema de servidor de aplicaciones, inicie sesión como `ibmadmin`.
   b. En una ventana de mandato, ejecute: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere Application Server.
   c. Si el mensaje `ADMU0509I: El servidor de aplicaciones "nodeagent" no es accesible. Parece estar detenido.` se visualiza, inicie el nodeagent utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "nodeagent" está STARTED.` . Si tuviera que iniciar el nodeagent, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor nodeagent abierto para e-business; el ID de proceso es 26654`.
   a. Si el mensaje `ADMU0509I: El servidor de aplicaciones "cpudServer1" no es accesible. Parece estar detenido.` se visualiza, inicie el cpdudServer1 utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startServer.sh cpudServer1`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "cpudServer1" está STARTED.` . Si tuviera que iniciar cpudServer1, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor cpudServer1 abierto para e-business; el ID de proceso es 26654`.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. cpudServer1

   Detenga los servidores en este orden:
   a. cpudServer1

b. nodeagent

El servidor cpudServer1 se detiene ejecutando el siguiente mandato en una ventana de mandatos de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS_ADMIN_PWD` donde *WAS_ADMIN_PWD* es la contraseña de administrador de WebSphere.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password CONTRAS_ADMIN_WAS`, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

4. Verifique que el servidor cpudServer1 se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos utilizando la WebSphere Application Server Administrative Console:
   a. Inicie sesión en la WebSphere Application Server Administrative Console en `http://HOST_SERVIDOR_APLICACIONES:9060/admin` utilizando el ID administrativo admin y la contraseña de WebSphere Application Server. *HOST_SERVIDOR_APLICACIONES* es el nombre de host para el servidor de aplicaciones.
   b. Vea el estado del servidor cpudServer1 pulsando **Servidores** > **Tipos de servidor** > **WebSphere Application Servers**.

      El icono de  significa que el servidor se ha iniciado. Si es necesario, seleccione el servidor y pulse **Reiniciar** para reiniciar el servidor.

      El icono de  significa que el servidor está detenido. Seleccione el servidor y haga clic en **Iniciar** para iniciar el servidor.

      El icono de  significa que el estado del servidor no está disponible. Puede que el agente del nodo no se esté ejecutando. Para iniciar el agente de nodo, ejecute el mandato `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh` en una ventana de mandatos.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. cpudServer1

   Detenga los servidores en este orden:
   a. cpudServer1
   b. nodeagent

   Para detener el servidor cpudServer, seleccione el servidor y pulse **Detener**.

   El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password CONTRAS_ADMIN_WAS`, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.
5. Verifique que se puede acceder a la consola de usuario de WebSphere UDDI Registry desde el sistema de WebSpherePortal, en servidor de aplicaciones, utilizando el siguiente URL: `http://HOST_SERVIDOR_APLICACIONES:9080/uddigui`. Donde *HOST_SERVIDOR_APLICACIONES* es el nombre de host para el servidor de aplicaciones.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Diagnóstico interno (Echo REST remoto)

La prueba de Diagnóstico interno (Echo REST remoto) prueba el acceso al programa de respuesta remoto accediendo a la URL. Este es un diagnóstico de Comprobación de verificación del sistema y comprueba los enlaces entre módulos Comprobación de verificación del sistema .

Recursos

La Diagnóstico interno (Echo REST remoto) utiliza los siguientes recursos:

- WebSphere Application Server (en servidor de aplicaciones).

Determinación de problemas

Si falla la prueba de Diagnóstico interno (Echo REST remoto) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de aplicaciones, revise los siguientes registros de configuración de WebSphere UDDI Registry:
      - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log`
2. Verifique que el sistema de archivos de servidor de aplicaciones no ha alcanzado su capacidad máxima. Esto puede determinarse mediante el mandato **`df -h`**.
3. Verifique que el servidor cpudServer1 se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos manuales:
   a. En el sistema de servidor de aplicaciones, inicie sesión como `ibmadmin`.
   b. En una ventana de mandato, ejecute: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere Application Server.
   c. Si el mensaje `ADMU0509I: El servidor de aplicaciones "nodeagent" no es accesible. Parece estar detenido.` se visualiza, inicie el nodeagent utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "nodeagent" está STARTED.` . Si tuviera que iniciar el nodeagent, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor nodeagent abierto para e-business; el ID de proceso es 26654`.
   a. Si el mensaje `ADMU0509I: El servidor de aplicaciones "cpudServer1" no es accesible. Parece estar detenido.` se visualiza, inicie el cpdudServer1 utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startServer.sh cpudServer1`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "cpudServer1" está STARTED.` . Si tuviera que iniciar cpudServer1, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor cpudServer1 abierto para e-business; el ID de proceso es 26654`.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. cpudServer1

   Detenga los servidores en este orden:

a. cpudServer1
b. nodeagent

El servidor cpudServer1 se detiene ejecutando el siguiente mandato en una ventana de mandatos de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password` *`WAS_ADMIN_PWD`* donde *WAS_ADMIN_PWD* es la contraseña de administrador de WebSphere.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

4. Verifique que el servidor cpudServer1 se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos utilizando la WebSphere Application Server Administrative Console:
   a. Inicie sesión en la WebSphere Application Server Administrative Console en `http://`*`HOST_SERVIDOR_APLICACIONES`*`:9060/admin` utilizando el ID administrativo admin y la contraseña de WebSphere Application Server. *HOST_SERVIDOR_APLICACIONES* es el nombre de host para el servidor de aplicaciones.
   b. Vea el estado del servidor cpudServer1 pulsando **Servidores** > **Tipos de servidor** > **WebSphere Application Servers**.

      El icono de  significa que el servidor se ha iniciado. Si es necesario, seleccione el servidor y pulse **Reiniciar** para reiniciar el servidor.

      El icono de  significa que el servidor está detenido. Seleccione el servidor y haga clic en **Iniciar** para iniciar el servidor.

      El icono de  significa que el estado del servidor no está disponible. Puede que el agente del nodo no se esté ejecutando. Para iniciar el agente de nodo, ejecute el mandato `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh` en una ventana de mandatos.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. cpudServer1

   Detenga los servidores en este orden:
   a. cpudServer1
   b. nodeagent

   Para detener el servidor cpudServer, seleccione el servidor y pulse **Detener**.

   El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.
5. Verifique que se puede acceder a la WebSphere UDDI User Console.
   a. En servidor de aplicaciones, acceda a: `https://`*`HOST_SERVIDOR_APLICACIONES`*`:9080/uddigui/`, donde *HOST_SERVIDOR_APLICACIONES* es el nombre de host de servidor de aplicaciones.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Mensajería (publicación/suscripción de tema de WebSphere Message Broker)

La prueba de Mensajería (publicación/suscripción de tema de WebSphere Message Broker) prueba las funciones de publicación y suscripción de WebSphere Message Broker. La prueba publica un mensaje para el tema con nombre JNDI listado en las propiedades como `jms/IopCatWmbPub`. WebSphere Message Broker recibe el mensaje, después publica un mensaje de retorno en el tema `IOP.CAT.PUB`. La prueba es satisfactoria si se recibe el mensaje de respuesta. La prueba falla si hay un error o si no se recibe el mensaje de respuesta dentro del tiempo de espera especificado en el archivo de propiedades.

Recursos

La prueba de Mensajería (publicación/suscripción de tema de WebSphere Message Broker) utiliza los siguientes recursos:

- WebSphere Portal Server (en servidor de aplicaciones).
- WebSphere Message Queue (en el servidor de sucesos).
- WebSphere Message Broker (en el servidor de sucesos).

Determinación de problemas

Si falla la prueba de Mensajería (publicación/suscripción de tema de WebSphere Message Broker) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Compruebe que haya conectividad de red entre el servidor de aplicaciones y el servidor de sucesos. Esto puede hacerse enviando mandatos **`ping`** con el nombre de host completo o corto a y desde cada servidor. Los resultados de los mandatos **`ping`** mostrarán si el DNS o el archivo `/etc/hosts` están resolviendo correctamente el nombre de host.
2. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verifique que los sistemas de archivos de servidor de sucesos yservidor de aplicaciones no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **`df -h`**.
4. Verifique que el gestor de colas de WebSphere Message Queue y el intermediario de WebSphere Message Broker se están ejecutando.
   a. En servidor de sucesos, inicie sesión como administrador de WebSphere Message Queue. Por ejemplo, `mqm`.
   b. En una ventana de mandato, ejecute **`source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq`**. Debería ver un mensaje similar al siguiente:
      ```
      QMNAME(IOC.MB.QM) STATUS(Running)
      ```
   c. Si se ha devuelto un estado distinto de `Running`, inicie el gestor de colas de WebSphere Message Queue utilizando el siguiente mandato: **`source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM`**.
   d. En servidor de sucesos, inicie sesión como administrador de WebSphere Message Broker. Por ejemplo, `mqm`.
   e. En una ventana de mandatos, ejecute **`source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist`**. Debería ver un mensaje similar al siguiente:
      ```
      BIP1284I: El intermediario 'IOC_BROKER' del gestor de colas 'IOC.MB.QM' se está ejecutando.
      ```
   f. Si se ha devuelto un estado distinto de `Running`, inicie el intermediario de WebSphere Message Broker utilizando el siguiente mandato: **`source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsistart IOC_BROKER`**.

5. Consulte los registros por si hay errores. Los registros se encuentran en servidor de sucesos en el directorio /var/log/messages. Busque mensajes con el prefijo 'BIP'. Busque también nombres de cola e indicaciones de fecha y hora a las que se ha ejecutado la prueba.
6. Si el intermediario o los gestores de colas no parecen haberse iniciado, también pueden iniciarse iniciando servidor de sucesos y ejecutando los scripts de inicio para el sistema.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Mensajería (publicación/suscripción de tema de WebSphere Message Queue)

La prueba Mensajería (publicación/suscripción de tema de WebSphere Message Queue) prueba las funciones de subscripción y publicación de WebSphere Message Queue. La prueba crea un tema especificado en las propiedades. A continuación publica un mensaje para el tema e intenta leer el mensaje publicado inmediatamente. La prueba tiene éxito si el mensaje enviado se puede leer. La prueba falla si hay un error o si no se puede leer el mensaje en 15 segundos (15.000 milisegundos).

Recursos

La prueba de Mensajería (publicación/suscripción de tema de WebSphere Message Queue) utiliza los siguientes recursos:

- WebSphere Portal Server (en servidor de aplicaciones).
- WebSphere Message Queue (en el servidor de sucesos).

Determinación de problemas

Si falla la prueba de Mensajería (publicación/suscripción de tema de WebSphere Message Queue) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Compruebe que hay conectividad de red entre servidor de aplicaciones y servidor de sucesos. Esto puede hacerse enviando mandatos **ping** con el nombre de host completo o corto a y desde cada servidor. Los resultados de los mandatos **ping** mostrarán si el DNS o el archivo /etc/hosts están resolviendo correctamente el nombre de host.
2. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
3. Verifique que los sistemas de archivos de los servidores no han alcanzado su capacidad máxima. Esto puede determinarse mediante el mandato **df -h**.
4. Verifique que el gestor de colas de WebSphere Message Queue se está ejecutando.
   a. En servidor de sucesos, inicie sesión como administrador de WebSphere Message Queue. Por ejemplo, mqm.
   b. En una ventana de mandato, ejecute **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. Debería ver un mensaje similar al siguiente:
      ```
      QMNAME(IOC.MB.QM) STATUS(Running)
      ```
   c. Si se ha devuelto un estado distinto de Running, inicie el gestor de colas de WebSphere Message Queue utilizando el siguiente mandato: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
5. Consulte los registros por si hay errores. Los registros se encuentran en servidor de sucesos en el directorio /var/log/messages. Busque mensajes con el prefijo 'BIP'. Busque también nombres de cola e indicaciones de fecha y hora a las que se ha ejecutado la prueba.

6. Si el gestor de colas no parece haberse iniciado, también puede iniciarse iniciando servidor de sucesos y ejecutando los scripts de inicio para el sistema.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Mensajería (comprobar de instalación de WebSphere Message Broker/Queue)

La prueba de Mensajería (comprobar de instalación de WebSphere Message Broker/Queue) determina si se puede acceder a WebSphere Message Queue y Message Broker. Esto se realiza mediante la ejecución del mandato WebSphere Message Broker **mqsilist** en el sistema que está ejecutando WebSphere Message Broker.

Recursos

La Mensajería (comprobar de instalación de WebSphere Message Broker/Queue) utiliza los siguientes recursos:

- WebSphere Portal Server (en servidor de aplicaciones).
- WebSphere Message Queue y Message Broker (en el servidor de sucesos).

Determinación de problemas

Si falla la prueba de Mensajería (comprobar de instalación de WebSphere Message Broker/Queue) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Compruebe que hay conectividad de red entre el sistema de portal WebSphere (en servidor de aplicaciones) y el sistema WebSphere Message Broker (en servidor de sucesos). Esto se puede hacer enviando los mandatos **ping** con el nombre de host completo o abreviado de servidor de sucesos desde servidor de aplicaciones y viceversa. Los resultados de los mandatos **ping** mostrarán si el DNS o el archivo `/etc/hosts` están resolviendo correctamente el nombre de host.
2. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verifique que los sistemas de archivo de los sistemas servidor de aplicaciones y servidor de sucesos no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **df -h**.
4. Verifique que el gestor de colas de WebSphere Message Queue y el intermediario de WebSphere Message Broker se están ejecutando.
   a. En servidor de sucesos, inicie sesión como administrador de WebSphere Message Queue. Por ejemplo, `mqm`.
   b. En una ventana de mandato, ejecute **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. Debería ver un mensaje similar al siguiente:
      ```
      QMNAME(IOC.MB.QM) STATUS(Running)
      ```
   c. Si se ha devuelto un estado distinto de `Running`, inicie el gestor de colas de WebSphere Message Queue utilizando el siguiente mandato: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
   d. En servidor de sucesos, inicie sesión como administrador de WebSphere Message Broker. Por ejemplo, `mqm`.
   e. En una ventana de mandatos, ejecute **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist**. Debería ver un mensaje similar al siguiente:
      ```
      BIP1284I: El intermediario 'IOC_BROKER' del gestor de colas 'IOC.MB.QM' se está ejecutando.
      ```

f. Si se ha devuelto un estado distinto de `Running`, inicie el intermediario de WebSphere Message Broker utilizando el siguiente mandato: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsistart IOC_BROKER**.

5. Consulte los registros por si hay errores. Los registros se encuentran en servidor de sucesos en el directorio `/var/log/messages`. Busque mensajes con el prefijo 'BIP'. Busque también nombres de cola e indicaciones de fecha y hora a las que se ha ejecutado la prueba.
6. Si el intermediario o los gestores de colas no parecen haberse iniciado, también pueden iniciarse iniciando servidor de sucesos y ejecutando los scripts de inicio para el sistema.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Mensajería (cola de WebSphere Message Broker/Queue)

La prueba de Mensajería (cola de WebSphere Message Broker/Queue) prueba la WebSphere Message Queue mediante la colocación de un mensaje en una cola.

Recursos

La prueba de Mensajería (cola de WebSphere Message Broker/Queue) utiliza los siguientes recursos:

- WebSphere Portal Server (en servidor de aplicaciones).
- WebSphere Message Queue (en el servidor de sucesos).
- WebSphere Message Broker (en el servidor de sucesos).

Determinación de problemas

Si falla la prueba de Mensajería (cola de WebSphere Message Broker/Queue) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Compruebe que hay conectividad de red entre servidor de aplicaciones y servidor de sucesos. Esto puede hacerse enviando mandatos **ping** con el nombre de host completo o corto a y desde cada servidor. Los resultados de los mandatos **ping** mostrarán si el DNS o el archivo `/etc/hosts` están resolviendo correctamente el nombre de host.
2. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verifique que los sistemas de archivo de los sistemas servidor de aplicaciones y servidor de sucesos no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **df -h**.
4. Verifique que el gestor de colas de WebSphere Message Queue y el intermediario de WebSphere Message Broker se están ejecutando.
   a. En servidor de sucesos, inicie sesión como administrador de WebSphere Message Queue. Por ejemplo, `mqm`.
   b. En una ventana de mandato, ejecute **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. Debería ver un mensaje similar al siguiente:
      ```
      QMNAME(IOC.MB.QM) STATUS(Running)
      ```
   c. Si se ha devuelto un estado distinto de `Running`, inicie el gestor de colas de WebSphere Message Queue utilizando el siguiente mandato: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
   d. En servidor de sucesos, inicie sesión como administrador de WebSphere Message Broker. Por ejemplo, `mqm`.

e. En una ventana de mandatos, ejecute **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist**. Debería ver un mensaje similar al siguiente:

```
BIP1284I: El intermediario 'IOC_BROKER' del gestor de colas 'IOC.MB.QM' se está ejecutando.
```

f. Si se ha devuelto un estado distinto de Running, inicie el intermediario de WebSphere Message Broker utilizando el siguiente mandato: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsistart IOC_BROKER**.

5. Consulte los registros por si hay errores. Los registros se encuentran en servidor de sucesos en el directorio /var/log/messages. Busque mensajes con el prefijo 'BIP'. Busque también nombres de cola e indicaciones de fecha y hora a las que se ha ejecutado la prueba.
6. Si el intermediario o los gestores de colas no parecen haberse iniciado, también pueden iniciarse iniciando servidor de sucesos y ejecutando los scripts de inicio para el sistema.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Supervisión (Netcool Impact Console)

La prueba Supervisión (Netcool Impact Console) determina si se está ejecutando la Netcool Impact Console y si se puede acceder a ella a través de la URL de Netcool Impact Console.

Recursos

La prueba de Supervisión (Netcool Impact Console) utiliza los siguientes recursos:

- Netcool Impact Server (en el servidor de sucesos)

Determinación de problemas

Si falla la prueba de Supervisión (Netcool Impact Console) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
   b. En servidor de sucesos, revise los siguientes registros de Netcool Impact:
      - /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemOut.log
      - /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemErr.log
2. Verifique que los sistemas de archivo del sistema servidor de sucesos no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **df -h**.
3. Verifique que el servidor server1 se ha iniciado.
   a. En el sistema servidor de sucesos inicie sesión como wasadmin.
   b. En una ventana de mandatos, ejecute: /opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/serverStatus.sh -all -username wasadmin -password *WAS_ADMIN_PWD* donde *WAS_ADMIN_PWD* es la contraseña del administrador deWebSphere Application Server.
   c. Si aparece el mensaje ADMU0509I: No se puede alcanzar el "server1" del servidor de aplicaciones. Parece estar detenido. inicie el servidor server1, que también iniciará Netcool Impact Console Server, utilizando el siguiente mandato: /opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/startServer.sh server1. Sáltese este paso si se visualiza el mensaje ADMU0508I: El servidor de aplicaciones "server1" está STARTED.. Si tuvo que iniciar el servidor server1, se mostrará un mensaje similar al siguiente: ADMU3000I: Servidor server1 abierto para e-business; el ID de proceso es 26654.

El servidor server1 se detiene ejecutando el siguiente mandato en una ventana de mandatos en servidor de sucesos: `/opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/stopServer.sh server1 -username wasadmin -password` *`WAS_ADMIN_PWD`* donde *WAS_ADMIN_PWD* es la contraseña de administrador deWebSphere .

4. Verifique que se puede acceder a Netcool Impact Console desde servidor de sucesos: `http://`*`EVENT_SERVER_HOST`*`:9080/nci` donde *EVENT_SERVER_HOST* es el nombre de host deservidor de sucesos.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Supervisión (Netcool Omnibus)

La prueba Supervisión (Netcool Omnibus) determina si Netcool Omnibus está disponible. Esto se realiza mediante la ejecución del mandato **`nco_pa_status -server NCO_PA`**.

Recursos

La prueba de Supervisión (Netcool Omnibus) utiliza los siguientes recursos:

- Netcool Omnibus Server (en el servidor de sucesos)

Determinación de problemas

Si falla la prueba de Supervisión (Netcool Omnibus) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Compruebe que haya conectividad de red entre el servidor de aplicaciones y el servidor de sucesos. Esto puede hacerse mediante el envío de mandatos de **`ping`** con el nombre de host abreviado y el completo de servidor de sucesos desde el servidor de aplicaciones . Los resultados de los mandatos **`ping`** mostrarán si el DNS o el archivo `/etc/hosts` están resolviendo correctamente el nombre de host.
2. Compruebe que los servicios del servidor de control de procesos y el agente se están ejecutando.
   a. Desde una ventana de mandatos en servidor de sucesos, ejecute el mandato **`$NCHOME/omnibus/bin/nco_pa_status -server NCO_PA`** como usuario *netcool* de Linux .
   b. Si los servicios no se han iniciado o no se están ejecutando, inicie el servidor ejecutando el mandato **`/etc/init.d/nco start`** enservidor de sucesos como usuario *root* de Linux .
   c. Si el agente de proceso no se está ejecutando, inicie el agente ejecutando el mandato **`$NCHOME/omnibus/bin/nco_pad`** enservidor de sucesos como usuario *netcool* de Linux .
3. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de sucesos, revise todos los registros que comiencen por NCO en los siguientes directorios:
      - `/opt/IBM/netcool/log`
      - `/opt/IBM/netcool/omnibus/log`
4. Verifique que los sistemas de archivo del sistema servidor de sucesos no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **`df -h`**.
5. Verifique que se puede acceder al portlet Netcool Omnibus desde servidor de aplicaciones: `http://`*`EVENT_SERVER_HOST`*`:9060/ibm/console` donde *EVENT_SERVER_HOST* es el nombre de host deservidor de sucesos.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Supervisión (Tivoli Composite Application Manager Agents - *servidor*)

La prueba de Supervisión (Tivoli Composite Application Manager Agents - *servidor*) prueba si los agentes de Tivoli Composite Application Manager se están ejecutando mediante la ejecución del mandato **cinfo**.

Recursos

La prueba de Supervisión (Tivoli Composite Application Manager Agents - *servidor*) utiliza los siguientes recursos:

- Tivoli Composite Application Manager
  - Agentes de Tivoli Composite Application Manager (en el servidor de aplicaciones)
  - Agentes de Tivoli Composite Application Manager (en el servidor de sucesos)
  - Agentes de Tivoli Composite Application Manager (en el servidor de datos)
  - Agentes de Tivoli Composite Application Manager (en el servidor de gestión)

Determinación de problemas

Si falla la prueba de Supervisión (Tivoli Composite Application Manager Agents - *servidor*) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Compruebe que existe conectividad de red entre servidor de aplicaciones, servidor de gestión, servidor de sucesos Y servidor de datos . Esto se puede realizar enviando mandatos de **ping** con con el nombre de host breve y completo de servidor de gestión, servidor de sucesos y servidor de datos desde el servidor de aplicaciones. Los resultados de los mandatos **ping** mostrarán si el DNS o el archivo `/etc/hosts` están resolviendo correctamente el nombre de host.
2. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verifique que los sistemas de archivo de los sistemas servidor de aplicaciones, servidor de gestión, servidor de sucesos y servidor de datos no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **df -h**.
4. Repita este paso en servidor de aplicaciones, servidor de gestión, servidor de sucesos y servidor de datos para verificar que los componentes de Tivoli Monitoring se están ejecutando.
   a. Inicie sesión en una sesión de terminal en el servidor como `root`.
   b. Ejecute el mandato **/opt/IBM/ITM/bin/cinfo -r**. Se mostrarán resultados similares a los siguientes. Los agentes serán diferentes en los distintos servidores. Los agentes deben tener un estado de ejecución.

```
********* Sun May 13 02:13:26 EDT 2012 *****************
User: root Groups: root bin daemon sys adm disk wheel idsldap tdsproxy ivmgr tivoli
Host name : baapp2 Installer Lvl:06.22.01.00
CandleHome: /opt/IBM/ITM
***********************************************************
Host    Prod    PID    Owner    Start    ID     ..Status
baapp2  lz      31042  root     May09    None   ...running
baapp2  ht      18755  root     May09    None   ...running
baapp2  yn      4190   root     02:11    None   ...running
```

   c. Inicie cualquier agente de Tivoli Composite Application Manager que no se esté ejecutando.
      1) Inicie sesión en una sesión de terminal en el servidor como `root`.
      2) Ejecute **/opt/IBM/ITM/bin/itmcmd agent start** *CÓDIGO_PRODUCTO*, donde *CÓDIGO_PRODUCTO* es el valor de ID de proceso correspondiente a un agente encontrado en los resultados del mandato **/opt/IBM/ITM/bin/cinfo -o**.

5. Revise los archivos de registro para las excepciones.
   a. En servidor de gestión, revise los siguientes registros de Tivoli Enterprise Monitoring Server y Tivoli Enterprise Portal Server:
      - Tivoli Enterprise Monitoring Server: `/opt/IBM/ITM/logs/*_CÓDIGO_PRODUCTO_{nnnnnnn}.log`
      - Tivoli Enterprise Portal Server: `/opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnnn}.log`

      donde *CÓDIGO_PRODUCTO* es el identificador de producto devuelto por el mandato **/opt/IBM/ITM/bin/cinfo -o**.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Supervisión (Tivoli Enterprise Monitoring Server)

La prueba de Supervisión (Tivoli Enterprise Monitoring Server) determina si el Tivoli Enterprise Monitoring Server que se ejecuta en el servidor de gestión está disponible. Se envía una consulta solicitando el estado del componente al servidor Tivoli Monitoring Web Services SOAP. La consulta incluye un ID de usuario y una contraseña no válida para el sistema. La respuesta debe indicar que se utilizó un ID de usuario y una contraseña no válida. El error indica que Tivoli Enterprise Monitoring Server está funcionando correctamente.

Recursos

La prueba de Supervisión (Tivoli Enterprise Monitoring Server) utiliza los siguientes recursos:

- Tivoli Enterprise Monitoring System (en el servidor de gestión)
  - Tivoli Monitoring Web Services SOAP Server
  - Tivoli Enterprise Portal Server
  - Base de datos de Tivoli Enterprise Portal Server DB2

Determinación de problemas

Si falla la prueba de Supervisión (Tivoli Enterprise Monitoring Server) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Compruebe que haya conectividad de red entre el servidor de aplicaciones y el servidor de gestión. Esto puede hacerse mediante el envío de mandatos de **ping** con el nombre de host abreviado y el completo de servidor de gestión desde el servidor de aplicaciones . Los resultados de los mandatos **ping** mostrarán si el DNS o el archivo `/etc/hosts` están resolviendo correctamente el nombre de host.
2. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de gestión, revise los siguientes registros de servidor de gestión:
      - Tivoli Event Monitoring Server: `/opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_ms_{nnnnnnn}.log`
      - Tivoli Event Portal Server: `/opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_cq_{nnnnnnn}.log`
      - Registros de WebSphere Application Server incorporado:
        - Registro de errores: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log`
        - Registro de salida: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log`

– Registro de inicio: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/startServer.log`

3. Verifique que los sistemas de archivo de servidor de gestión no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **df -h**.
4. Verifique que los componentes de supervisión de Tivoli se están ejecutando en servidor de gestión.
   a. Inicie sesión en una sesión de terminal en servidor de gestión como `root`.
   b. Ejecute el mandato **/opt/IBM/ITM/bin/cinfo -r**.
5. Verifique que las bases de datos de componentes de Tivoli son operativas.
   a. Inicie sesión en una sesión de terminal en servidor de gestión como`db2inst1`.
   b. Ejecute el mandato **ps -ef | grep db2inst1**.
   c. Verifique que se están ejecutando los procesos de DB2 . Incluyen db2sysc, db2vend y db2acd.
   d. Si no se están ejecutando los procesos de DB2 , ejecute el mandato **$> db2start** .
   e. Compruebe los registros de DB2 en servidor de datos para obtener los errores de base de datos relacionados que inician las bases de datos utilizadas por los componentes Tivoli . Se pueden encontrar los archivos de registro en el directorio `/datahome/db2inst1/sqllib/db2dump` en servidor de datos.
6. en los resultados, verifique que se está ejecutando Tivoli Enterprise Monitoring Server buscando una entrada para `ms`. Si no está listada la entrada, no se está ejecutando Tivoli Enterprise Monitoring Server.
7. Si Tivoli Enterprise Monitoring Server no se está ejecutando, inicie el servidor.
   a. Inicie sesión en una sesión de terminal en servidor de gestión como `root`.
   b. Ejecute el mandato **/opt/IBM/ITM/bin/itmcmd server start HUB_MWOS** .
8. En los resultados del paso 4, verifique que Tivoli Enterprise Portal Server se está ejecutando buscando una entrada para `cq`. Si la entrada no está listada, no se está ejecutando Tivoli Enterprise Portal Server.
9. Si no se está ejecutando Tivoli Enterprise Portal Server, inicie el servidor.
   a. Inicie sesión en una sesión de terminal en servidor de gestión como `root`.
   b. Ejecute el mandato **/opt/IBM/ITM/bin/itmcmd agent start cq** .
10. En los resultados del paso 4, verifique que se están ejecutando los demás subcomponentes válidos.

Tabla 79. Componentes de Tivoli

Componente	Descripción
`kf`	Eclipse Help Server
`cq`	Tivoli Enterprise Portal Server
`lz`	Agente de supervisión para el SO Linux
`ms`	Servidor de Tivoli Enterprise Monitoring
`yn`	IBM Tivoli Composite Application Manager Agent for WebSphere Applications

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Supervisión (WebSphere Business Monitor Business Space Console)

La prueba Supervisión (WebSphere Business Monitor Business Space Console) determina si se puede acceder a WebSphere Business Monitor Business Space utilizando la URL de HTTP de WebSphere Business Monitor Business Space.

Recursos

La prueba de Supervisión (WebSphere Business Monitor Business Space Console) utiliza los siguientes recursos:

- WebSphere Application Server (en servidor de aplicaciones).

Determinación de problemas

Si la prueba de Supervisión (WebSphere Business Monitor Business Space Console) no tiene éxito, realice lo siguiente para encontrar y resolver el problema de acceso.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de aplicaciones, revise los siguientes registros de WebSphere Business Monitor:
      - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log`
2. Verifique que los sistemas de archivo del sistema servidor de aplicaciones no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **`df -h`**.
3. Verifique que el servidor de WebSphere Business Monitor se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos manuales:
   a. En el sistema de servidor de aplicaciones, inicie sesión como `ibmadmin`.
   b. En una ventana de mandato, ejecute: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere Application Server.
   c. Si el mensaje `ADMU0509I: El servidor de aplicaciones "nodeagent" no es accesible. Parece estar detenido.` se visualiza, inicie el nodeagent utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "nodeagent" está STARTED.` . Si tuviera que iniciar el nodeagent, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor nodeagent abierto para e-business; el ID de proceso es 26654`.
   a. Si el mensaje `ADMU0509I: El servidor de aplicaciones "WBM_DE.AppTarget.WBMNode1.0" no es accesible. Parece estar detenido.` se visualiza, inicie WBM_DE.AppTarget.WBMNode1.0 utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startServer.sh WBM_DE.AppTarget.WBMNode1.0`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "WBM_DE.AppTarget.WBMNode1.0" está STARTED.` . Si tuviera que iniciar WBM_DE.AppTarget.WBMNode1.0, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor WBM_DE.AppTarget.WBMNode1.0 abierto para e-business; el ID de proceso es 26654`.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. WBM_DE.AppTarget.WBMNode1.0

   Detenga los servidores en este orden:
   a. WBM_DE.AppTarget.WBMNode1.0

b. nodeagent

El servidor WBM_DE.AppTarget.WBMNode1.0 se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopServer.sh WBM_DE.AppTarget.WBMNode1.0 -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`* donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

4. Verifique que el servidor de WebSphere Business Monitor se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos utilizando la WebSphere Application Server Administrative Console:
   a. Inicie sesión en la WebSphere Application Server Administrative Console en `http://`*`HOST_SERVIDOR_APLICACIONES`*`:9060/admin` utilizando el ID administrativo admin y la contraseña de WebSphere Application Server. *HOST_SERVIDOR_APLICACIONES* es el nombre de host para servidor de aplicaciones.
   b. Vea el estado del servidor WBM_DE.AppTarget.WBMNode1.0 pulsando **Servidores** > **Tipos de servidor** > **WebSphere Application Servers**.

      El icono de  significa que el servidor se ha iniciado. Si es necesario, seleccione el servidor y pulse **Reiniciar** para reiniciar el servidor.

      El icono de  significa que el servidor está detenido. Seleccione el servidor y haga clic en **Iniciar** para iniciar el servidor.

      El icono de  significa que el estado del servidor no está disponible. Puede que el agente del nodo no se esté ejecutando. Para iniciar el agente de nodo, ejecute el mandato `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh` en una ventana de mandatos.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:
   a. nodeagent
   b. WBM_DE.AppTarget.WBMNode1.0

   Detenga los servidores en este orden:
   a. WBM_DE.AppTarget.WBMNode1.0
   b. nodeagent

   Para detener el servidor WBM_DE.AppTarget.WBMNode1.0, seleccione el servidor y pulse **Detener**.

   El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.
5. Verifique que se puede acceder a WebSphere Business Monitor Business Space desde el sistema WebSphere Portal, en servidor de aplicaciones, utilizando la siguiente URL: `http://`*`APPLICATION_SERVER_HOST`*`:9084/BusinessSpace`. Donde *HOST_SERVIDOR_APLICACIONES* es el nombre de host para el servidor de aplicaciones.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Supervisión (WebSphere Business Monitor Mobile Device Console)

La prueba Supervisión (WebSphere Business Monitor Mobile Device Console) determina si se puede acceder aWebSphere Business Monitor Mobile utilizando la URL de HTTP de WebSphere Business Monitor Mobile.

Recursos

La prueba de Supervisión (WebSphere Business Monitor Mobile Device Console) utiliza los siguientes recursos:

- WebSphere Application Server (en servidor de aplicaciones).

Determinación de problemas

Si la prueba de Supervisión (WebSphere Business Monitor Mobile Device Console) no tiene éxito, realice lo siguiente para encontrar y resolver el problema de acceso.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de aplicaciones, revise los siguientes registros de WebSphere Business Monitor:
      - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log`
2. Verifique que los sistemas de archivo del sistema servidor de aplicaciones no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **`df -h`**.
3. Verifique que el servidor de WebSphere Business Monitor se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos manuales:
   a. En el sistema de servidor de aplicaciones, inicie sesión como `ibmadmin`.
   b. En una ventana de mandato, ejecute: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere Application Server.
   c. Si el mensaje `ADMU0509I: El servidor de aplicaciones "nodeagent" no es accesible. Parece estar detenido.` se visualiza, inicie el nodeagent utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "nodeagent" está STARTED.` . Si tuviera que iniciar el nodeagent, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor nodeagent abierto para e-business; el ID de proceso es 26654`.
   a. Si el mensaje `ADMU0509I: El servidor de aplicaciones "WBM_DE.AppTarget.WBMNode1.0" no es accesible. Parece estar detenido.` se visualiza, inicie WBM_DE.AppTarget.WBMNode1.0 utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startServer.sh WBM_DE.AppTarget.WBMNode1.0`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "WBM_DE.AppTarget.WBMNode1.0" está STARTED.` . Si tuviera que iniciar WBM_DE.AppTarget.WBMNode1.0, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor WBM_DE.AppTarget.WBMNode1.0 abierto para e-business; el ID de proceso es 26654`.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:

a. nodeagent
b. WBM_DE.AppTarget.WBMNode1.0

Detenga los servidores en este orden:

a. WBM_DE.AppTarget.WBMNode1.0
b. nodeagent

El servidor WBM_DE.AppTarget.WBMNode1.0 se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopServer.sh WBM_DE.AppTarget.WBMNode1.0 -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`* donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

4. Verifique que el servidor de WebSphere Business Monitor se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos utilizando la WebSphere Application Server Administrative Console:
   a. Inicie sesión en la WebSphere Application Server Administrative Console en `http://`*`HOST_SERVIDOR_APLICACIONES`*`:9060/admin` utilizando el ID administrativo admin y la contraseña de WebSphere Application Server. *HOST_SERVIDOR_APLICACIONES* es el nombre de host para servidor de aplicaciones.
   b. Vea el estado del servidor WBM_DE.AppTarget.WBMNode1.0 pulsando **Servidores** > **Tipos de servidor** > **WebSphere Application Servers**.

      El icono de  significa que el servidor se ha iniciado. Si es necesario, seleccione el servidor y pulse **Reiniciar** para reiniciar el servidor.

      El icono de  significa que el servidor está detenido. Seleccione el servidor y haga clic en **Iniciar** para iniciar el servidor.

      El icono de  significa que el estado del servidor no está disponible. Puede que el agente del nodo no se esté ejecutando. Para iniciar el agente de nodo, ejecute el mandato `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh` en una ventana de mandatos.

Importante: Los servidores deben iniciarse y detenerse en un orden específico.

Inicie los servidores en este orden:

a. nodeagent
b. WBM_DE.AppTarget.WBMNode1.0

Detenga los servidores en este orden:

a. WBM_DE.AppTarget.WBMNode1.0
b. nodeagent

Para detener el servidor WBM_DE.AppTarget.WBMNode1.0, seleccione el servidor y pulse **Detener**.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de aplicaciones: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password` *`CONTRAS_ADMIN_WAS`*, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

5. Verifique que se puede acceder a WebSphere Business Monitor Mobile desde el sistema de portal de WebSphere , en servidor de aplicaciones , utilizando la siguiente URL: `http://`*`APPLICATION_SERVER_HOST`*`:9084/mobile`. Donde *HOST_SERVIDOR_APLICACIONES* es el nombre de host para el servidor de aplicaciones.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Política (Tivoli Service Request Manager Maximo Console)

La prueba de Política (Tivoli Service Request Manager Maximo Console) determina si se puede acceder a Tivoli Service Request ManagerMaximo utilizando la página del centro de inicio de Tivoli Service Request ManagerMaximo.

Recursos

La prueba de Política (Tivoli Service Request Manager Maximo Console) utiliza los siguientes recursos:

- Tivoli Service Request Manager Maximo (en servidor de sucesos).

Determinación de problemas

Si la prueba de Política (Tivoli Service Request Manager Maximo Console) no tiene éxito, realice lo siguiente para encontrar y resolver el problema de acceso.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de sucesos, revise los siguientes registros de Tivoli Service Request Manager:
      - `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log`
2. Verifique que los sistemas de archivo de los sistemas servidor de sucesos y servidor de aplicaciones no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **`df -h`**.
3. Compruebe que el servidor de Tivoli Service Request Manager se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos manuales:
   a. En el sistema de servidor de sucesos, inicie sesión como `ibmadmin`.
   b. En una ventana de mandatos, ejecute: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/serverStatus.sh -all -username waswebadmin -password` *`CONTRASEÑA_ADMIN_WAS`* donde *CONTRASEÑA_ADMIN_WAS* es la contraseña de administrador de WebSphere Application Server.
   c. Si el mensaje `ADMU0509I: El servidor de aplicaciones "nodeagent" no es accesible. Parece estar detenido.` se visualiza, inicie el nodeagent utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startNode.sh`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "nodeagent" está STARTED.` . Si tuviera que iniciar el nodeagent, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor nodeagent abierto para e-business; el ID de proceso es 26654`.
   a. Si el mensaje `ADMU0509I: El servidor de aplicaciones "MXServer1" no es accesible. Parece estar detenido.` se visualiza, inicie MXServer1 utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startServer.sh MXServer1`. Omita este paso si se visualiza el mensaje `ADMU0508I: El servidor de aplicaciones "MXServer1" está STARTED.` . Si tuviera que iniciar MXServer1, se visualizará un mensaje similar al siguiente: `ADMU3000I: Servidor MXServer1 abierto para e-business; el ID de proceso es 26654`.

   Importante: Los servidores deben iniciarse y detenerse en un orden específico.

   Inicie los servidores en este orden:

   a. nodeagent

b. MXServer1

Detenga los servidores en este orden:

a. MXServer1

b. nodeagent

El servidor MXServer1 se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de sucesos: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopServer.sh MXServer1 -username waswebadmin -password CONTR_ADMIN_WAS`, donde *CONTR_ADMIN_WAS* es la contraseña del administrador de WebSphere.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de sucesos: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopNode.sh -username waswebadmin -password CONTRAS_ADMIN_WAS`, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

4. Compruebe que el servidor de Tivoli Service Request Manager se ha iniciado. La verificación se puede realizar utilizando la WebSphere Application Server Administrative Console o mediante pasos manuales. Los siguientes son los pasos utilizando la WebSphere Application Server Administrative Console:

   a. Inicie sesión en la WebSphere Application Server Administrative Console en `http://HOST_SERVIDOR_SUCESOS:9061/admin` utilizando el ID administrativo admin y la contraseña de WebSphere Application Server. *HOST_SERVIDOR_SUCESOS* es el nombre de host para servidor de sucesos.

   b. Vea el estado del servidor MXServer1 pulsando **Servidores** > **Tipos de servidor** > **WebSphere Application Servers**.

      El icono de  significa que el servidor se ha iniciado. Si es necesario, seleccione el servidor y pulse **Reiniciar** para reiniciar el servidor.

      El icono de  significa que el servidor está detenido. Seleccione el servidor y haga clic en **Iniciar** para iniciar el servidor.

      El icono de  significa que el estado del servidor no está disponible. Puede que el agente del nodo no se esté ejecutando. Para iniciar el agente de nodo, ejecute el mandato `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startNode.sh` en una ventana de mandatos.

Importante: Los servidores deben iniciarse y detenerse en un orden específico.

Inicie los servidores en este orden:

a. nodeagent

b. MXServer1

Detenga los servidores en este orden:

a. MXServer1

b. nodeagent

Para detener el servidor MXServer1, seleccione el servidor y pulse **Detener**.

El nodeagent se detiene ejecutando el siguiente mandato en una ventana de mandato de servidor de sucesos: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopNode.sh -username waswebadmin -password CONTRAS_ADMIN_WAS`, donde *CONTRAS_ADMIN_WAS* es la contraseña del administrador de WebSphere.

5. Verifique que se puede acceder a la página Tivoli Service Request Manager Maximo Start Center desde el sistema de portal de WebSphere , en servidor de sucesos, utilizando la siguiente URL: `http://EVENT_SERVER_HOST:31015/maximo/ui/login`. Donde *HOST_SERVIDOR_SUCESOS* es el nombre de host del servidor de sucesos. El ID de usuario es `maxadmin`.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Seguridad (Tivoli Access Manager)

La prueba Seguridad (Tivoli Access Manager) determina si se está ejecutando Tivoli Access Manager enviando un mandato **pd_start** desdeservidor de gestión y verificando los resultados.

Recursos

La prueba de Seguridad (Tivoli Access Manager) utiliza los siguientes recursos:

- Tivoli Access Manager incluyendo los servidores de autorización y políticas (en servidor de gestión)

Determinación de problemas

Si falla la prueba de Seguridad (Tivoli Access Manager) , haga lo siguiente para encontrar y resolver el problema.

Acerca de esta tarea

En los pasos siguientes, pdmgrd es el Tivoli Access Manager Authorization Server, pdmgrproxyd es el Policy Proxy Server y webseald-default es el Tivoli Access Manager WebSEAL Server.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de gestión revise los siguientes registros de Tivoli Access Manager:
      - `/var/PolicyDirector/log/msg__pdmgrd_utf8.log`
      - `/var/PolicyDirector/log/msg__pdacld_utf8.log`
   b. En servidor de aplicaciones revise los siguientes registros de Tivoli Access Manager:
      - `/var/pdweb/log/msg__*.log` donde * es cualquier valor.
      - `/var/pdweb/log/config_data__*.log` donde * es cualquier valor.
2. Verifique que los sistemas de archivo de los sistemas servidor de gestión y servidor de aplicaciones no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **df -h**.
3. Verifique que los componentes de Tivoli Access Manager se estén ejecutando.
   a. Inicie sesión en una sesión de terminal en servidor de gestión como `root`.
   b. Ejecute el mandato **pd_start status**. Los resultados serán similares a los siguientes:

```
Servidores de Tivoli Access Manager

Servidor        Habilitado Ejecutando
-----------------------------------
pdmgrd           sí         sí
pdacld           sí         sí
pdmgrproxyd      no        no
```

   c. Si los servidores pdmgrd o pdacld no se están ejecutando, inícielos mediante la ejecución de mandato **pd_start start**.

      Nota: Solo los servidores pdmgrd y pdacld están habilitados en servidor de gestión. Ambos se inician con el mandato **pd_start start** y ambos se pueden detener con el mandato **pd_start stop**.
4. Verifique que se están ejecutando los componentes necesarios de Tivoli Access Manager WebSEAL.
   a. Inicie sesión en una sesión de terminal en servidor de aplicaciones como root.
   b. Ejecute el mandato **pd_start status**. Los resultados serán similares a los siguientes:

```
Servidores de Tivoli Access Manager

Servidor        Habilitado Ejecutando
```

```
---------------------------------
pdmgrd           no         no
pdacld           no         no
pdmgrproxyd      no         no
webseald-default sí         sí
```

c. Si el servidor webseald-default no se está ejecutando, inícielo mediante la ejecución de mandato **pd_start start**.

Nota: Solo el servidor webseald-default está habilitado en servidor de aplicaciones. Se inicia con el mandato **pd_start start** y se puede detener con el mandato **pd_start stop**.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Seguridad (Tivoli Access Manager Web Portal Manager)

La prueba de Seguridad (Tivoli Access Manager Web Portal Manager) determina si se puede acceder a la aplicación Tivoli Access Manager Web Portal por medio de la URL de la aplicación Tivoli Access Manager Web Portal.

Recursos

La prueba de Seguridad (Tivoli Access Manager Web Portal Manager) utiliza los siguientes recursos:

- Tivoli Access Manager Server (en servidor de gestión).

Determinación de problemas

Si la prueba de Seguridad (Tivoli Access Manager Web Portal Manager) no tiene éxito, realice lo siguiente para encontrar y resolver el problema de acceso.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de WebSphere Portal:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. En servidor de gestión, revise los siguientes registros de Tivoli Access Manager - WebSphere Portal Manager:
      - `/opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log`
2. Verifique que los sistemas de archivo del sistema servidor de gestión no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **df -h**.
3. Verifique que se ha iniciado Tivoli Access Manager - Web Portal Manager.
   a. En el servidor de gestión, inicie sesión como `ibmadmin`.
   b. En una ventana de mandatos, ejecute: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/serverStatus.sh -all -username waswebadmin -password` *WAS_ADMIN_PWD* donde *WAS_ADMIN_PWD* es la contraseña de administrador de WebSphere Application Server.
   c. Si aparece el mensaje `ADMU0509I: No se ha podido alcanzar el "dmgr" del servidor de aplicaciones. Parece estar detenido.` , inicie dmgr utilizando el siguiente mandato: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/startManager.sh` . Sáltese este paso si aparece el mensaje `ADMU0508I: el "dmgr" del servidor de aplicaciones está INICIADO.` se muestra. Si tuvo que iniciar el dmgr, se mostrará un mensaje similar al siguiente: `ADMU3000I: dmgr de servidor abierto para e-business; el ID de proceso es 26654`.

   El WebSphere Application Server Deployment Manager, incluyendo Tivoli Access Manager - Web Portal Manager, se detiene ejecutando el siguiente mandato en una ventana de mandatos en servidor

de gestión: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/stopManager.sh -username waswebadmin -password` *WAS_ADMIN_PWD* donde *WAS_ADMIN_PWD* es la contraseña del administrador de WebSphere .

4. Compruebe que se puede acceder al Tivoli Access Manager - Web Portal Manager desde el sistema de WebSphere Portal.
   a. En el servidor de gestión, acceda al siguiente URL: `http://`*HOST_SERVIDOR_GESTIÓN*`9060/admin`. donde *HOST_SERVIDOR_GESTIÓN* es el nombre de host para servidor de gestión.
   b. Pulse **Tivoli Access Manager** > **Web Portal Manager** > **Usuarios** > **Buscar usuarios**.
   c. Inicie sesión utilizando como usuario `sec_master`.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Seguridad (WebSEAL Console)

La prueba Seguridad (WebSEAL Console) determina si Tivoli Access Manager y Tivoli Access Manager WebSEAL se están ejecutando con los recursos necesarios accediendo a la URL de WebSEAL HTTP en el puerto 80 y comprobando la página devuelta para la cadena "Intelligent Operations Center".

Recursos

La prueba de Seguridad (WebSEAL Console) utiliza los siguientes recursos:

- Tivoli Access Manager incluyendo los servidores de autorización y políticas (en servidor de gestión)
- Tivoli Access Manager WebSEAL (en servidor de aplicaciones)

Determinación de problemas

Si falla la prueba de Seguridad (WebSEAL Console) , haga lo siguiente para encontrar y resolver el problema.

Acerca de esta tarea

En los pasos siguientes, pdmgrd es el Tivoli Access Manager Authorization Server, pdmgrproxyd es el Policy Proxy Server y webseald-default es el Tivoli Access Manager WebSEAL Server.

Procedimiento

1. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de gestión revise los siguientes registros de Tivoli Access Manager:
      - `/var/PolicyDirector/log/msg__pdmgrd_utf8.log`
      - `/var/PolicyDirector/log/msg__pdacld_utf8.log`
   b. En servidor de aplicaciones revise los siguientes registros de Tivoli Access Manager:
      - `/var/pdweb/log/msg__*.log` donde * es cualquier valor.
      - `/var/pdweb/log/config_data__*.log` donde * es cualquier valor.
2. Verifique que los sistemas de archivo de los sistemas servidor de gestión y servidor de aplicaciones no han alcanzado la capacidad. Esto puede determinarse mediante el mandato **`df -h`**.
3. Verifique que los componentes de Tivoli Access Manager se estén ejecutando.
   a. Inicie sesión en una sesión de terminal en servidor de gestión como `root`.
   b. Ejecute el mandato **`pd_start status`**. Los resultados serán similares a los siguientes:

```
Servidores de Tivoli Access Manager

Servidor        Habilitado Ejecutando
```

```
----------------------------------
pdmgrd           sí         sí
pdacld           sí         sí
pdmgrproxyd      no        no
```

c. Si los servidores pdmgrd o pdacld no se están ejecutando, inícielos mediante la ejecución de mandato **pd_start start**.

Nota: Solo los servidores pdmgrd y pdacld están habilitados en servidor de gestión. Ambos se inician con el mandato **pd_start start** y ambos se pueden detener con el mandato **pd_start stop**.

4. Verifique que se están ejecutando los componentes necesarios de Tivoli Access Manager WebSEAL.
   a. Inicie sesión en una sesión de terminal en servidor de aplicaciones como root.
   b. Ejecute el mandato **pd_start status**. Los resultados serán similares a los siguientes:

```
Servidores de Tivoli Access Manager

Servidor        Habilitado Ejecutando
----------------------------------
pdmgrd           no         no
pdacld           no         no
pdmgrproxyd      no         no
webseald-default sí         sí
```

   c. Si el servidor webseald-default no se está ejecutando, inícielo mediante la ejecución de mandato **pd_start start**.

Nota: Solo el servidor webseald-default está habilitado en servidor de aplicaciones. Se inicia con el mandato **pd_start start** y se puede detener con el mandato **pd_start stop**.

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Servidor web (IBM HTTP Server Console)

La prueba de Servidor web (IBM HTTP Server Console) prueba el acceso al servidor HTTP de IBM accediendo a la URL del servidor HTTP de IBM .

Recursos

La Servidor web (IBM HTTP Server Console) utiliza los siguientes recursos:

- Servidor HTTP de IBM (en servidor de aplicaciones).

Determinación de problemas

Si falla la prueba de Servidor web (IBM HTTP Server Console) , haga lo siguiente para encontrar y resolver el problema.

Procedimiento

1. Compruebe que hay conectividad de red a servidor de aplicaciones. Esto se puede hacer enviando mandatos **ping** con el nombre de host completo o corto de servidor de aplicaciones. Los resultados de los mandatos **ping** mostrarán si el DNS o el archivo `/etc/hosts` están resolviendo correctamente el nombre de host.
2. Revise los archivos de registro para ver si hay excepciones de tiempo de ejecución.
   a. En servidor de aplicaciones, revise los siguientes registros de IBM HTTP:
      - `/opt/IBM/HTTPServer/logs/error_log`
      - `/opt/IBM/HTTPServer/logs/access_log`
3. Verifique que el sistema de archivos de servidor de aplicaciones no ha alcanzado su capacidad máxima. Esto puede determinarse mediante el mandato **df -h**.

4. Compruebe que se puede acceder a la página predeterminada de IBM HTTP Server desde el sistema de WebSphere Portal.
   a. En servidor de aplicaciones, acceda a: `https://APPLICATION_SERVER_HOST:82/` donde*APPLICATION_SERVER_HOST* es el nombre de host de servidor de aplicaciones.
   b. Si no se puede acceder a la página predeterminada, ejecute el mandato **ps -ef | grep HTTPServer** para determinar qué procesos del servidor HTTP de IBM se están ejecutando. Los procesos de servidor HTTP de IBM comienzan por `/opt/IBM/HTTPServer/bin/httpd`. Habrá siete procesos.
   c. Si alguno, pero no todos los procesos se están ejecutando, detenga los procesos que se están ejecutando antes de reiniciar todos los procesos.
      1) En servidor de aplicaciones, inicie sesión como `root`.
      2) Cambie al directorio `/opt/IBM/HTTPServer/bin` .
      3) Ejecute los siguientes mandatos para detener todos los procesos de IBM HTTP en ejecución:
         ```
         ./apachectl stop
         ./adminctl stop
         ```
      4) Verifique que todos los procesos se han detenido ejecutando el mandato **ps -ef | grep HTTPServer** .
      5) Si cualquiera de los procesos del servidor HTTP de IBM aún se está ejecutando, deténgalos utilizando**kill -9** *pid* donde *pid* es el identificador de proceso del proceso de servidor HTTP deIBM .
   d. Si los procesos del servidor HTTP no se está ejecutando, inicie los componentes del servidor HTTP de IBM .
      1) En el servidor de aplicaciones, inicie la sesión como `root`.
      2) Cambie al directorio `/opt/IBM/HTTPServer/bin` .
      3) Ejecute los siguientes mandatos para iniciar todos los procesos HTTP de IBM que se están ejecutando:
         ```
         ./adminctl start
         ./apachectl start
         ```
      4) Verifique que todos los procesos se han iniciado ejecutando el mandato **ps -ef | grep HTTPServer** .

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Flujo de sucesos de Intelligent Operations Center

La prueba Flujo de sucesos de Intelligent Operations Center verifica si los componentes críticos relacionados con procesos de sucesos de IBM Intelligent Operations Center funcionan como se esperaba. Esto se realiza simulando sucesos externos y determinando si los resultados son como se esperaba.

Recursos

La prueba de Flujo de sucesos de Intelligent Operations Center utiliza los siguientes recursos:

- IBM WebSphere Message Broker (en el servidor de aplicaciones).
- IBM WebSphere Message Queue (en el servidor de aplicaciones).
- IBM Netcool/OMNIbus (en el servidor de sucesos).
- IBM Netcool/Impact (en servidor de sucesos).
- IBM DB2 (en servidor de datos).

Determinación de problemas

Si la prueba de Flujo de sucesos de Intelligent Operations Center no tiene éxito, realice lo siguiente para encontrar y resolver el problema de acceso.

Procedimiento

1. Compruebe que los componentes de IBM Intelligent Operations Center se están ejecutando.
   a. En una ventana de mandato de servidor de gestión, ejecute **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status all** *contraseña*, donde *contraseña* es la contraseña del administrador de IBM Intelligent Operations Center definida cuando IBM Intelligent Operations Center se desplegó.
   b. Si hay componentes que no se estén ejecutando, inicie dichos componentes ejecutando **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start** *ID_componente contraseña*, donde *contraseña* es la contraseña del administrador de IBM Intelligent Operations Center definida cuando IBM Intelligent Operations Center se desplegó, e *ID_componente* es un ID indicado en `Opciones de destino` al ejecutar **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh help**.
2. Revise el registro de Netcool/OMNIbus (`/opt/IBM/netcool/omnibus/log/ioc_xml.log`) en servidor de sucesos para ver si hay algún error.
3. Si es necesario, inicie la sonda de Tivoli Netcool/OMNIbus mediante la ejecución de lo siguiente en servidor de sucesos.

```
mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Prueba de Flujo de notificaciones de Intelligent Operations Center

La prueba Flujo de notificaciones de Intelligent Operations Center verifica si los componentes críticos relacionados con los procesos de notificación de IBM Intelligent Operations Center están funcionando como se esperaba. Esto se realiza simulando notificaciones externas y determinando si los resultados son como se esperaba.

Recursos

La prueba de Flujo de notificaciones de Intelligent Operations Center utiliza los siguientes recursos:

- IBM WebSphere Message Queue (en el servidor de aplicaciones).
- IBM Netcool/OMNIbus (en el servidor de sucesos).
- IBM Netcool/Impact (en servidor de sucesos).
- IBM DB2 (en servidor de datos).

Determinación de problemas

Si la prueba de Flujo de notificaciones de Intelligent Operations Center no tiene éxito, realice lo siguiente para encontrar y resolver el problema de acceso.

Procedimiento

1. Compruebe que los componentes de IBM Intelligent Operations Center se están ejecutando.
   a. En una ventana de mandato de servidor de gestión, ejecute **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status all** *contraseña*, donde *contraseña* es la contraseña del administrador de IBM Intelligent Operations Center definida cuando IBM Intelligent Operations Center se desplegó.
   b. Si hay componentes que no se estén ejecutando, inicie dichos componentes ejecutando **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start** *ID_componente contraseña*, donde *contraseña* es la contraseña del administrador de IBM Intelligent Operations Center definida cuando IBM Intelligent Operations Center se desplegó, e *ID_componente* es un ID indicado en `Opciones de destino` al ejecutar **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh help**.
2. Revise el registro de Netcool/OMNIbus (`/opt/IBM/netcool/omnibus/log/ioc_xml.log`) en servidor de sucesos para ver si hay algún error.
3. Si es necesario, inicie la sonda de Tivoli Netcool/OMNIbus mediante la ejecución de lo siguiente en servidor de sucesos.

```
mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```

Qué hacer a continuación

Resuelva los problemas o errores encontrados y reintente la prueba.

Capítulo 7. Mantenimiento de la solución

Lleve a cabo las tareas descritas en esta sección para mantener la solución funcionando sin problemas.

Copia de seguridad de datos

Para evitar la pérdida de datos valioso en IBM Intelligent Operations Center, realice una copia de seguridad de determinados archivos, directorios y bases de datos a intervalos regulares.

Al ampliar IBM Intelligent Operations Center, se recomienda desarrollar un procedimiento de copia de seguridad para los elementos añadidos, por ejemplo:

- Informes
- Bases de datos auxiliares
- Tablas de base de datos
- Análisis personalizados
- Portlets
- Aplicaciones Java

Tenga en cuenta también los datos acumulados, por ejemplo:

- Datos de la base de datos Common Access Protocol (CAP)
- Datos de la base de datos IBM WebSphere Business Monitor
- Datos de registro de usuario de Lightweight Directory Access Protocol (LDAP)
- Datos del sistema de información geográfica (GIS)

Adopte una convención de nomenclatura para facilitar la identificación de las ampliaciones añadidas. En general, realice un seguimiento de los datos creados o acumulados desde que instaló la solución original. Implemente procedimientos para realizar copias de seguridad de los datos y que, cuando actualice la solución, no pierda datos valiosos.

Copia de seguridad de bases de datos

La tabla siguiente lista las bases de datos de las cuales se recomienda realizar una copia de seguridad en IBM Intelligent Operations Center.

Tabla 80. Bases de datos IBM Intelligent Operations Center

Servicio o componente	Instancia de base de datos	Nombres de base de datos	Servidor
Base de datos de Intelligent Operations Center	db2inst1	• IOCDB	Servidor de datos
Portal	db2inst2	• CUSTDB • FDBKDB • LKMDDB • JCRDB • COMMDB • RELDB	Servidor de datos
Business Intelligence	db2inst3	• CXLOGDB • CXCONTDB	Servidor de datos

Tabla 80. Bases de datos IBM Intelligent Operations Center (continuación)

Servicio o componente	Instancia de base de datos	Nombres de base de datos	Servidor
Reglas empresariales y supervisión de actividad empresarial	db2inst4	• UDDIDB • WODMDCDB • MONITOR • WBMDB • RESDB	Servidor de datos
Modelo semántico	db2inst5	• JTS • IIC	Servidor de datos
Gestión de solicitudes de servicio	db2inst6	• MÁXIMO	Servidor de datos
Gestión de identidades	db2inst7	• TIMDB	Servidor de datos
Aplicaciones	db2inst8	• LDAPDB • LDAPDB2B	Servidor de datos

Creación de instantáneas de infraestructura virtual

La mayoría de las infraestructuras tienen una función de instantánea que conserva el estado y los datos del entorno virtual en un momento específico. Se recomienda encarecidamente que tome una instantánea del entorno antes de realizar cambios importantes. Existen muchas herramientas de gestión de infraestructura virtual disponibles, la mayoría de las cuales tienen su propia función de implementación de instantáneas. Es importante familiarizarse con requisitos e instrucciones específicos sobre cómo realizar copias de seguridad correctamente en el entorno virtual leyendo con atención las instrucciones de la guía del administrador proporcionadas por el proveedor de infraestructura virtual.

Tareas relacionadas:

"Copia de seguridad antes de personalizar KPI" en la página 176
Realice copias de seguridad y restaure los KPI creados o modificados con IBM WebSphere Business Monitor o con el portlet de Indicadores clave de rendimiento.

Información relacionada:

IBM Smarter Cities Software Solutions Redbooks

Ajuste del rendimiento

Las seccione siguientes describen cómo ajustar servidor de aplicaciones y WebSphere Application Server.

Información relacionada:

IBM Websphere Portal V 7.0 Guía de ajuste de rendimiento

Information Center de IBM Websphere Application Server, Network Deployment, Versión 7.0

Ajuste de servidor de aplicaciones

Acerca de esta tarea

Utilice las siguientes directrices, que se basan en los resultados de pruebas de rendimiento, para establecer el tamaño de almacenamiento dinámico de la máquina virtual Java .

Procedimiento

1. Establezca los tamaños de almacenamiento dinámico mínimo y máximo en los mismos valores.

2. Establezca el tamaño de almacenamiento dinámico en un valor compatible con la memoria física y que esté por encima de 2 GB.

Qué hacer a continuación

Para obtener más información, consulte el enlace relacionado que figura al final de este tema.

Ajuste de WebSphere Application Server

Para obtener información sobre cómo ajustar el rendimiento de WebSphere Application Server Versión 7, consulte el enlace relacionado al final de este tema.

Gestión de archivos de registro

IBM Intelligent Operations Center almacena archivos de registro en varias ubicaciones diferentes. Para evitar problemas de rendimiento del sistema, archive periódicamente los archivos de registro y elimine los archivos de registro originales.

Si no gestiona los archivos de registro y el número aumenta de forma indefinida, los archivos de registro pueden llegar a llenar una partición del sistema de archivos. Llenar una partición de sistemas de archivos puede tener consecuencias negativas y hacer que el sistema se detenga.

Para obtener información acerca de los archivos de registro que están disponibles enIBM Intelligent Operations Center, consulte el enlace al final del tema.

Conceptos relacionados:

"Resolución de problemas de los componentes" en la página 306
Puede utilizar la herramienta Comprobación de verificación del sistema para resolver los problemas de los componentes en IBM Intelligent Operations Center.

Actualización de la señal LTPA para un inicio de sesión único

IBM Intelligent Operations Center utiliza una señal Lightweight Third-Party Authentication (LTPA) para habilitar el inicio de sesión único entre muchos servicios. La señal y las claves generadas durante la instalación no caducan. Es una buena práctica de seguridad volver a generar periódicamente la señal LTPA y actualizar los servicios utilizándola.

Antes de empezar

Se debe instalar el producto IBM Intelligent Operations Center y todos los servicios iniciados antes de actualizar la señal LTPA.

Este procedimiento requiere que se detengan y se inicien todos los servicios, así no se tiene que hacer la actualización mientras el sistema está en producción. Cualquier usuario que haya iniciado sesión en el sistema experimentará una interrupción del servicio y puede perder datos.

Procedimiento

Genere una nueva señal LTPA para servidor de aplicaciones

1. En servidor de aplicaciones , abra un navegador web y vaya a `http://application_host:9060/ibm/console` donde *application_host* es el nombre de host de servidor de aplicaciones.
2. Inicie sesión como usuario `webwasadmin` con la contraseña especificada en el parámetro `WAS.ADMIN.ACCOUNT.PWD` del archivo de propiedades de topología.
3. Pulse **Seguridad** > **Seguridad global** > **Mecanismos de autenticación y caducidad** > **LTPA** > **Generar claves**.

4. Entre una contraseña dos veces para la nueva señal LTPA. La contraseña se utiliza para cifrar la señal LTPA. La contraseña se utilizará al importar la señal LTPA. Registre la contraseña del parámetro `WAS.LTPA.PWD` en el archivo de propiedades de topología.
5. Entre la vía de acceso y el nombre de archivo donde se guardará la señal LTPA, por ejemplo, `/tmp/newapp.ltpa`. Si especifica una vía de acceso o nombre de archivo diferente, sustituya la vía de acceso o el nombre de archivo por `/tmp/newapp.ltpa` en el resto de pasos.
6. Pulse **Exportar claves**. La nueva señal LTPA se guarda como `/tmp/newapp.ltpa`.
7. Pulse **Mensajes** > **Guardar**. Se guardarán las actualizaciones. Ignore cualquier aviso sobre un dominio de inicio de sesión único que no se está definiendo.

Copie la nueva señal LTPA a servidor de sucesos.

8. En servidor de aplicaciones, inicie sesión como usuario `root` y abra una ventana de terminal.
9. Ejecute el mandato **cp /tmp/newapp.ltpa /tmp/stproxy.ltpa** . Esto reemplaza al archivo que se creó cuando se instaló IBM Intelligent Operations Center .
10. Ejecute el mandato **scp /tmp/newapp.ltpa root@***event_host* **:/tmp/newapp.ltpa** donde *event_host* es el nombre de host de servidor de sucesos. Al solicitárselo, entre la contraseña de `root` para servidor de sucesos. La señal LTPA se copia a servidor de sucesos.

Importe la nueva señal LTPA

11. En servidor de sucesos abra un navegador web y vaya a `http://event_host:9061/ibm/console` donde *event_host* es el nombre de host completo deservidor de sucesos.
12. Inicie sesión como usuario `webwasadmin` con la contraseña especificada en el parámetro `TSRM.WAS.ADMIN.PWD` del archivo de propiedades de topología.
13. Pulse **Seguridad** > **Proteger administración, aplicaciones e infraestructura** > **Mecanismos y caducidad de la autenticación**.
14. Entre la contraseña para la señal LTPA y `/tmp/newapp.ltpa` para el nombre de archivo.
15. Pulse **Importar claves**.
16. Pulse **Mensajes** > **Guardar**. Se guardarán las actualizaciones.

Genere una nueva señal LTPA para servidor de sucesos

17. Pulse **Mecanismos de autenticación y caducidad** > **Generar claves**.
18. Entre una contraseña dos veces para la nueva señal LTPA. La contraseña se utilizará al importar la señal LTPA.
19. Entre la vía de acceso y el nombre de archivo donde se guardará la señal LTPA, por ejemplo, `/tmp/newevent.ltpa`. Si especifica una vía de acceso o nombre de archivo diferente, sustituya la vía de acceso o el nombre de archivo por `/tmp/newevent.ltpa` en el resto de pasos.
20. Pulse **Exportar claves**. La nueva señal LTPA se guarda como `/tmp/newevent.ltpa`.

Copie la nueva señal LTPA de servidor de sucesos a servidor de aplicaciones.

21. En servidor de aplicaciones, inicie sesión como usuario `root` y abra una ventana de terminal.
22. Ejecute el mandato **scp /tmp/newevent.ltpa root@***event_host* **:/tmp/newevent.ltpa** donde *event_host* es el nombre de host de servidor de sucesos. Al solicitárselo, entre la contraseña de `root` para servidor de sucesos. La señal LTPA se copia a servidor de sucesos.

Actualice el servicio de seguridad con la nueva señal LTPA.

23. En servidor de aplicaciones inicie sesión como usuario `root` y abra una ventana de terminal.
24. Ejecute el mandato **cp /tmp/newapp.ltpa /opt/pdweb/etc/** .
25. Ejecute el mandato **cp /tmp/newevent.ltpa /opt/pdweb/etc/** .
26. Cree un archivo de mandato llamado `/tmp/pd.com` que contenga los siguientes mandatos:

```
server task default-webseald-host_aplicación create -t tcp -h host_aplicación -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stwebclient
server task default-webseald-host_aplicación create -t tcp -h host_aplicación -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stbaseapi
server task default-webseald-host_aplicación create -t tcp -h host_aplicación -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stwebapi
server task default-webseald-host_aplicación create -t tcp -h host_aplicación -p 9081 -b
supply -c iv-user,iv-creds -i -j -f -J trailer -A -2 -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw
/cognosserver task default-webseald-host_aplicación create -t tcp -h host_suceso -p 82 -i
-j -f -J trailer -A -2 -F /opt/pdweb/etc/newevent.ltpa -Z eventLTPApw /tsrm
```

Donde:

host_aplicación
es el nombre de host completo de servidor de aplicaciones.

event_host
es el nombre de host completo de servidor de sucesos.

appLTPApw
es la contraseña especificada al crear la señal LTPA para servidor de aplicaciones.

eventLTPApw
es la contraseña especificada al crear la señal LTPA para servidor de sucesos.

27. Ejecute el mandato **/opt/PolicyDirector/bin/pdadmin -a sec_master -p** *contraseña* **/ tmp/pd.com** donde *contraseña* es la contraseña definida en el parámetro TAM.WEBSEAL.ADMIN.PWD del archivo de propiedades de topología.

Actualice el inicio de sesión único para el servicio de colaboración.

28. Siga los pasos en "Configuración del inicio de sesión único para servicios de colaboración" en la página 54 para actualizar el inicio de sesión único para el servicio de colaboración.

Detenga y reinicie todos los servicios.

29. Utilizando Herramienta de control de plataforma detenga todos los servicios.
30. Utilizando Herramienta de control de plataforma inicie todos los servicios. Las señales LTPA se propagarán a todos los servicios.

Sugerencias de mantenimiento

Las sugerencias adicionales para el mantenimiento de la solución se documentan en forma de notas técnicas individuales en IBM Support Portal.

El siguiente enlace inicia una consulta personalizada de la base de conocimiento de soporte para todas las versiones de IBM Intelligent Operations Center: Ver todos los consejos de mantenimiento de IBM Intelligent Operations Center.

Capítulo 8. Mediante la interfaz de solución

IBM Intelligent Operations Center es una solución basada en web que utiliza tecnología de portal. Puede acceder a la solución con cualquiera de los navegadores web soportados.

Para obtener información sobre los navegadores web soportados, siga al enlace situado al final del tema.

Información relacionada:

Navegadores soportados para IBM Intelligent Operations Center

Iniciar sesión

Inicie sesión en la interfaz de usuario de IBM Intelligent Operations Center.

Antes de empezar

Póngase en contacto con el administrador local para obtener un ID de usuario y una contraseña. El administrador es responsable de asegurarse que disponga del nivel de acceso de seguridad adecuado a su rol en la organización. El administrador también el proporcionará el URL de la dirección web para acceder al portal de la solución.

Acerca de esta tarea

Utilice el siguiente procedimiento para iniciar una nueva sesión del navegador y acceder a la IBM Intelligent Operations Center . También puede acceder a la solución desde otros IBM Smarter Cities Software Solutions instalado en su entorno. En la barra de navegación principal en la parte superior del portal, seleccione **Intelligent Operations Center**.

Procedimiento

1. Especifique el URL en el campo de dirección del navegador.

   Nota: En el URL, es necesario el nombre de dominio completo, por ejemplo, `http://application_server_hostname/wpsv70/wps/myportal`. Si utiliza la dirección IP, en lugar del dominio registrado completo, algunos portlets no se visualizarán correctamente.
2. En la página de inicio de sesión, especifique el ID de usuario y la contraseña.
3. Pulse **Iniciar sesión**.

Resultados

Solo se mostrarán las páginas, las características y los datos para los que tenga permiso de acceso. Póngase en contacto con el administrador si necesita más acceso.

Tareas relacionadas:

"Cierre de sesión"
Cierre sesión para salir de interfaz de usuario de IBM Intelligent Operations Center y finalizar la sesión con el servidor. De forma predeterminada, el enlace **Finalizar sesión** se encuentra en la esquina superior derecha de IBM Intelligent Operations Center.

Cierre de sesión

Cierre sesión para salir de interfaz de usuario de IBM Intelligent Operations Center y finalizar la sesión con el servidor. De forma predeterminada, el enlace **Finalizar sesión** se encuentra en la esquina superior derecha de IBM Intelligent Operations Center.

Tareas relacionadas:

"Iniciar sesión" en la página 271
Inicie sesión en la interfaz de usuario de IBM Intelligent Operations Center.

Visualización o edición de su perfil de usuario

Puede ver o cambiar la información de su perfil de usuario para IBM Intelligent Operations Center.

Acerca de esta tarea

El perfil contiene la información entrada previamente por el administrador. Puede actualizar el perfil editando la información en el campo de atributos. Por ejemplo, puede cambiar la contraseña existente por una nueva.

Tabla 81. Atributos del perfil de usuario IBM Intelligent Operations Center

Atributo	Descripción	¿El usuario puede editar?
ID de usuario*	Se asigna un ID a cada nuevo usuario por parte del administrador por motivos de identificación.	No
Contraseña*	Se asigna una contraseña por parte del administrador por seguridad. La contraseña debe ser exclusiva y tener de 5 a 60 caracteres de longitud. Las contraseñas válidas deben contener sólo los caracteres a-z, A-Z, punto ".", guión "-" y subrayado "_ ".	Sí
Nombre	El nombre de pila, o nombre dado se puede introducir por el administrador o el usuario.	Sí
Apellido*	El apellido o nombre de familia lo entra el administrador.	Sí
Correo electrónico	La dirección de correo electrónico la puede entrar el administrador o el usuario.	Sí

Nota: Los atributos marcados con un asterisco son necesarios para la correcta creación de un usuario nuevo. mientras que los atributos sin marcar con un asterisco son opcionales.

Procedimiento

1. A la derecha de la barra de navegación superior, seleccione **Editar mi perfil**. Se muestran los atributos para el perfil.
2. Para cambiar la contraseña:
   a. Especifique su contraseña actual (el texto de la contraseña no se muestra).
   b. En el campo **Nueva contraseña** y en los campos **Confirmar contraseña** , entre la nueva contraseña.
3. Escriba o edite la información en cualquiera de los campos restantes.
4. Para enviar los campos, pulse **Aceptar**.

Resultados

El perfil de usuario se actualiza con los cambios.

Uso de páginas

Una página consta de uno o más portlets complementarios. Mediante IBM Intelligent Operations Center, se puede interactuar con los portlets de una página para acceder a la información que se necesita y responder a sucesos como sea necesario.

IBM Intelligent Operations Center ofrece seis vistas de páginas de muestra diferentes.

Si dispone de acceso de administrador, en la vista de página, puede acceder al servicio del portal para gestionar las páginas. Podrá editar páginas o crear una página nueva. Haga clic a la derecha de la pestaña de nombre de la página y seleccione una opción en el menú de la página.Para obtener más información, siga el enlace situado al final de este tema.

Tareas relacionadas:

"Creación o personalización de una página" en la página 149
Para crear páginas nuevas que se incluyan en IBM Intelligent Operations Center y especificar qué portlets mostrar en esas páginas. Puede personalizar la apariencia y el diseño de los portlets incluidos en cada página.

Vista Supervisor: Estado

Utilice la vista Supervisor: Estado para obtener una vista consolidada de los indicadores clave de rendimiento (KPI) y los sucesos claves. La vista Supervisor: Estado permite a usuarios con responsabilidad en toda la organización supervisar, gestionar y responder a cambios de estado en relación a áreas clave de bienestar y rendimiento organizativo.

La vista Supervisor: Estado es una página web interactiva. La página contiene los portlets listados en Tabla 82. Los portlets son secciones independientes de la página que cooperan entre sí para proporcionar información e interacción completas en el nivel ejecutivo.

Tabla 82. Portlets de la vista Supervisor: Estado

Portlet	Descripción
"Estado" en la página 297	El portlet Estado proporciona un resumen de nivel ejecutivo del estado de los ICR en las organizaciones que tienen permiso para ver. Utilice este portlet para ver cambios actualizados en el estado de ICR para poder planificar y tomar medidas si es necesario.
"Obtención de detalles de indicador clave de rendimiento" en la página 281	Para centrarse en un categoría de ICR específica en el portlet Obtención de detalles de indicador clave de rendimiento, haga clic en la categoría en el portlet Estado. Luego esta categoría se muestra en solitario en el portlet Obtención de detalles de indicador clave de rendimiento. Puede utilizar la lista para inspeccionar los ICR subyacentes hasta llegar a los detalles del ICR que causara el cambio de estado.

Tabla 82. Portlets de la vista Supervisor: Estado (continuación)

Portlet	Descripción
"Notificaciones" en la página 293	El portlet Notificaciones proporciona una lista dinámica e interactiva de las alertas que resultan de cambios en ICR y sucesos relacionados. El papel de este portlet es llamar la atención sobre los cambios en ICR o en estado de sucesos. La lista contiene detalles clave de cada una de las alertas.Por ejemplo, cuando un KPI cambia el estado de amarillo a rojo, se envía una alerta al portlet Notificaciones .
"Mis actividades" en la página 290	Un usuario que haya iniciado sesión puede ver las actividades asignadas a ellos en el portlet Mis actividades. En el portlet Mis actividades, las actividades se agrupan por sus procedimientos de operación estándar de nivel superior. Cada procedimiento operativo estándar se corresponde con un suceso individual.
"Contactos" en la página 277	El portlet Contactos puede mostrar una lista de contactos organizados por categoría. Puede organizarlas los contactos en categorías basadas en las personas con las que tiene que comunicarse. Por ejemplo, puede tener una categoría para contactos de trabajo generales y otra categoría para contactos de trabajo de un proyecto concreto. Con el portlet Contactos, puede comunicarse con la gente y modificar su estado en línea, sus contactos o sus grupos.

Vista Supervisor: Operaciones

Utilice la vista Supervisor: Operaciones para obtener una visión general de los acontecimientos a medida que se producen. La vista Supervisor: Operaciones está dirigida a supervisores y gestores que supervisan sucesos actuales y planifican sucesos futuros.

La vista Supervisor: Operaciones es una página web interactiva. La página contiene los portlets listados en Tabla 83. Los portlets son secciones independientes de la página que cooperan entre sí para proporcionar información e interacción completas en el nivel de gestión.

Tabla 83. Portlets de la vista Supervisor: Operaciones

Portlet	Descripción
"Mapa" en la página 285	Un mapa de la región geográfica con marcadores de sucesos y recursos. Un formulario de filtro para seleccionar las categorías de los sucesos que se muestran en el mapa y en los portlets enlazados con el portlet Mapa. Un formulario de filtro para seleccionar las prestaciones de los recurso que se muestran en el mapa y en la pestaña **Recursos**, en el portlet Detalles enlazado. Para ver este formulario, seleccione primero **Ver recursos de la zona** en el portlet Detalles .
"Detalles" en la página 278	El portlet Detalles es un portlet de lista interactivo. Todos los sucesos que está autorizado a ver son visibles en la lista de sucesos y en cualquier portlet de mapa vinculado al portlet Detalles.

Tabla 83. Portlets de la vista Supervisor: Operaciones (continuación)

Portlet	Descripción
"Notificaciones" en la página 293	El portlet Notificaciones proporciona una lista dinámica e interactiva de las alertas que resultan de cambios en ICR y sucesos relacionados. El papel de este portlet es llamar la atención sobre los cambios en ICR o en estado de sucesos. La lista contiene detalles clave de cada una de las alertas.Por ejemplo, cuando se producen incidentes relacionados en un área definida, se envía una alerta al portlet de Notificaciones.
"Mis actividades" en la página 290	Un usuario que haya iniciado sesión puede ver las actividades asignadas a ellos en el portlet Mis actividades. En el portlet Mis actividades, las actividades se agrupan por sus procedimientos de operación estándar de nivel superior. Cada procedimiento operativo estándar se corresponde con un suceso individual.
"Contactos" en la página 277	El portlet Contactos puede mostrar una lista de contactos organizados por categoría. Puede organizarlas los contactos en categorías basadas en las personas con las que tiene que comunicarse. Por ejemplo, puede tener una categoría para contactos de trabajo generales y otra categoría para contactos de trabajo de un proyecto concreto. Con el portlet Contactos, puede comunicarse con la gente y modificar su estado en línea, sus contactos o sus grupos.

Vista Operador: Operaciones

Utilice la vista de Operador: Operaciones para mantener el conocimiento de sucesos y su ubicación. La vista Operador: Operaciones está destinada a operadores, gestores u otros que supervisen y respondan a los sucesos actuales.

La vista Operador: Operaciones es una página web interactiva. La página contiene los portlets listados en Tabla 84. Los portlets son secciones independientes de la página que cooperan entre sí para proporcionar información e interacción completas en el nivel de las operaciones.

Tabla 84. Portlets de la vista Operador: Operaciones

Portlet	Descripción
"Mapa" en la página 285	Un mapa de la región geográfica con marcadores de sucesos y recursos. Un formulario de filtro para seleccionar las categorías de los sucesos que se muestran en el mapa y en los portlets enlazados con el portlet Mapa. Un formulario de filtro para seleccionar las prestaciones de los recurso que se muestran en el mapa y en la pestaña **Recursos**, en el portlet Detalles enlazado. Para ver este formulario, seleccione primero **Ver recursos de la zona** en el portlet Detalles .
"Detalles" en la página 278	El portlet Detalles es un portlet de lista interactivo. Todos los sucesos que está autorizado a ver son visibles en la lista de sucesos y en cualquier portlet de mapa vinculado al portlet Detalles.
"Notificaciones" en la página 293	El portlet Notificaciones proporciona una lista dinámica e interactiva de las alertas que resultan de cambios en ICR y sucesos relacionados. El papel de este portlet es llamar la atención sobre los cambios en ICR o en estado de sucesos. La lista contiene detalles clave de cada una de las alertas. Por ejemplo, cuando dos sucesos graves se producen cerca uno del otro en ubicación y tiempo se envía una alerta al portlet Notificaciones .

Tabla 84. Portlets de la vista Operador: Operaciones (continuación)

Portlet	Descripción
"Mis actividades" en la página 290	Un usuario que haya iniciado sesión puede ver las actividades asignadas a ellos en el portlet Mis actividades. En el portlet Mis actividades, las actividades se agrupan por sus procedimientos de operación estándar de nivel superior. Cada procedimiento operativo estándar se corresponde con un suceso individual.
"Contactos" en la página 277	El portlet Contactos puede mostrar una lista de contactos organizados por categoría. Puede organizarlas los contactos en categorías basadas en las personas con las que tiene que comunicarse. Por ejemplo, puede tener una categoría para contactos de trabajo generales y otra categoría para contactos de trabajo de un proyecto concreto. Con el portlet Contactos, puede comunicarse con la gente y modificar su estado en línea, sus contactos o sus grupos.

Supervisor: informes

Utilice la vista Supervisor: informes para ver un resumen de los datos de suceso generados a partir de la ejecución de informes predefinidos. También puede utilizar la vista Supervisor: informes para crear informes personalizados o configurar informes predefinidos. Estos informes está destinados a operadores, gestores u otros que supervisen sucesos actuales y planifiquen los futuros.

La vista de Supervisor: informes es una página web interactiva que contiene distintos informes basados en datos seleccionados que proporcionan información e interacción completas en el nivel de supervisor. Esta información se muestra en los gráficos que resumen los datos de suceso que está en el sistema.

En la vista Supervisor: informes , puede configurar y ver los informes de los portlets "Informes " en la página 294. De forma predeterminada, alguno de los portlets Informes muestra informes de ejemplo.

Operador: informes

Utilice la vista Operador: informes para mantener la conciencia de informes, sucesos y alertas. La vista Operador: informes está destinada a operadores, gestores u otros que supervisen sucesos.

La vista Operador: informes proporciona un resumen de datos de suceso generados por la ejecución de informes predefinidos. También puede utilizar la vista Operador: informes para visualizar informes personalizados. Estos informes ayudan a supervisar sucesos actuales, tomar medidas para gestionar sucesos y planear sucesos futuros.

La vista Operador: informes es una página web interactiva. Puede elegir ver varios informes diferentes que proporcionan información e interacción completa a nivel de operador.

En la vista Operador: informes , puede configurar y ver los informes de los portlets "Informes " en la página 294. De forma predeterminada, alguno de los portlets Informes muestra informes de ejemplo.

Vista Mapa de ubicación

Utilice la vista de Mapa de ubicación para mantener el conocimiento de sucesos y su posición en un mapa de ubicación. La vista Mapa de ubicación está destinada a operadores, gestores u otros que supervisen y respondan a los sucesos actuales.

La vista Mapa de ubicación es una página web interactiva. La página contiene los portlets listados en Tabla 85 en la página 277. Los portlets son secciones independientes de la página que cooperan entre sí para proporcionar información e interacción completas en el nivel de las operaciones.

Tabla 85. Portlets de la vista Mapa de ubicación

Portlet	Descripción
"Mapa de ubicación" en la página 282	Un diagrama de la ubicación con marcadores para sucesos. Un formulario de filtro para seleccionar las categorías de los sucesos que se muestran en el mapa. Una lista de los mapas de ubicación disponibles organizados por clasificación.
"Detalles" en la página 278	El portlet Detalles es un portlet de lista interactivo. Todos los sucesos que está autorizado a ver son visibles en la lista de sucesos y en cualquier portlet de mapa vinculado al portlet Detalles.

Uso de los portlets

Un portlet proporciona acceso a información que se puede ver y con la que se puede interactuar en una página de portal.

IBM Intelligent Operations Center ofrece varios portlets diferentes.

Para obtener ayuda sobre el uso de cada portlet, haga clic en la esquina superior derecha del portlet y seleccione **Ayuda** en el menú que aparece.

Para cambiar el tamaño de un portlet, haga clic en la esquina superior derecha del portlet y seleccione las opciones del menú que se muestra, de la siguiente manera:

- Para ampliar el portlet para que ocupe toda la página, haga clic en **Maximizar**.
- Para ocultar el contenido del portlet, excepto la barra de título, haga clic en **Minimizar**.
- Para restaurar un portlet minimizado o maximizado a la vista predeterminada, haga clic en **Restaurar** .

Administrador

Personalización de un portlet

Como administrador puede cambiar los valores del portlet pulsando en la esquina superior derecha del portlet y seleccionando una opción en el menú de dicho portlet.

Hay dos modos posibles de personalización, y ambos cambian los valores de portlet para todos los usuarios:

- **Editar valores compartidos** cambia el portlet únicamente para la instancia de dicho portlet en la que se encuentre cuando cambie los valores.
- **Configurar** cambia los valores globales del portlet para todas las instancias de dicho portlet, allí donde dichas instancias aparezcan.

Los modos de personalización que están disponibles dependen de los permisos asociados con el ID de usuario. Los valores globales son reemplazados por los valores compartidos.

Los portlets que se suministran con IBM Intelligent Operations Center tienen valores específicos de un tipo de portlet, como por ejemplo la definición del nivel de zoom predeterminado de un mapa. Además, puede configurar parámetros de portlet genéricos que son comunes a todos los portlets suministrados, como por ejemplo, el título de portlet.

Contactos

Utilice el portlet Contactos para enviar mensajes instantáneos dentro de la solución.

El portlet Contactos puede mostrar una lista de contactos organizados por categoría. Puede organizarlas los contactos en categorías basadas en las personas con las que tiene que comunicarse. Por ejemplo,

puede tener una categoría para contactos de trabajo generales y otra categoría para contactos de trabajo de un proyecto concreto. Con el portlet Contactos, puede comunicarse con la gente y modificar su estado en línea, sus contactos o sus grupos.

Haga clic en los menús de la parte superior del portlet:

- **Archivo** para añadir contactos, modificar grupos o finalizar sesión.
- **Herramientas** para configurar una charla, una reunión o un anuncio, o para cambiar la configuración de privacidad.
- **Ayuda** para obtener información más detallada sobre cómo utilizar el portlet.

Haga clic en su estado para modificar el estado y el mensaje. El estado predeterminado indica que está disponible. Puede cambiar el estado para indicar que está alejado del sistema, en una reunión o que no quiere que le molesten.

El estado de los usuarios que han iniciado sesión se visualiza en el portlet Contactos. Si un usuario que ha iniciado sesión cierra la ventana del navegador o finaliza la sesión en WebSphere Portal, el estado de dicho usuario todavía se visualiza como conectado hasta que la sesión caduque. Sin embargo, los mensajes que se envían a este usuario, después de que el usuario haya cerrado la ventana del navegador o finalizado la sesión, no se entregan. Por lo tanto, se muestra un mensaje de error al usuario que intenta enviar el mensaje. Para asegurarse de que el estado se actualice de inmediato en el portlet Contactos, cierre sesión pulsando **Archivo** > **Finalizar sesión**.

Nota: Para que este portlet funcione como se espera, debe iniciar sesión en el portal de soluciones mediante el nombre de dominio completo del Servidor de aplicaciones de IBM Intelligent Operations Center. Si inicia sesión en el portal utilizando una dirección IP o un alias de nombre de host, en lugar del nombre de dominio completo registrado, este portlet no se mostrará correctamente.

Administrador

Si tiene acceso de administrador, puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Los valores que puede cambiar en el portlet Contactos son:

- Archivo de ayuda
- Altura del portlet
- Altura del portlet cuando se maximiza.
- Título del portlet
- Paquete de recursos

Referencia relacionada:

“Valores del portlet Contactos” en la página 151
Personalice el portlet Contactos cambiando los valores en los campos de la ventana **Valores compartidos** .

Detalles

Utilice el portlet Detalles para visualizar, supervisar y gestionar sucesos en IBM Intelligent Operations Center.

El portlet Detalles es un portlet de lista interactivo. Todos los sucesos que está autorizado a ver son visibles en la lista de sucesos y en cualquier portlet de mapa vinculado al portlet Detalles.

Recursos en las proximidades de un suceso se pueden visualizar en una lista de recursos y en un mapa.

Sucesos y recursos

El portlet Detalles tiene dos elementos de interfaz interactivos, como se muestra en la siguiente tabla:

Tabla 86. Visualización del portlet Detalles

Elemento de la interfaz	Descripción
Sucesos e incidencias	La lista de sucesos contiene detalles clave para cada uno de los sucesos. Puede visualizar una descripción más detallada de un suceso desplazando el cursor sobre la fila de la lista.
Recursos	Los detalles clave sobre los recursos en las cercanías de un red inteligente se muestran cuando se hace clic con el botón derecho en el suceso seleccionado. Puede ver una descripción más detallada de un recurso pasando el cursor sobre la fila de la lista.

Inicialmente, cuando abre IBM Intelligent Operations Center , el portlet Detalles muestra todos los sucesos relevantes.

En el portlet Mapa , selecciona las categorías de sucesos y prestaciones de recursos que se van a mostrar. Las categorías de sucesos que se muestran en la pestaña **Sucesos e incidencias** y en el portlet Mapa son los mismos. Las prestaciones de los recursos mostradas en la pestaña **Recursos** y en el portlet Mapa son las mismas.

La lista de sucesos se renueva de forma regular con nuevos sucesos y actualizaciones, sujeta a los filtros definidos para limitar las categorías que se muestran.

Un contador en la esquina izquierda de la barra de acciones al final de la lista indica el número de elementos visualizados y el número total de elementos. En el centro de la barra de acciones, puede seleccionar el número de elementos que se visualizarán al mismo tiempo. Si hay más filas que se pueden visualizar a la vez, puede desplazarse hacia adelante o hacia atrás haciendo clic en los botones de la esquina derecha de la barra de acciones.

Propiedades de suceso

La siguiente tabla resume las propiedades que describen un suceso:

Tabla 87. Propiedades de suceso

Propiedad	Contenido
Quién	
Remitente	Origen o ID de usuario
Nombre de la persona de contacto	Persona con la que ponerse en contacto para obtener información adicional.
Correo electrónico de contacto	Dirección de correo electrónico de la persona de contacto.
Teléfono de contacto	Número de teléfono de la persona de contacto
Qué	
Tipo de suceso*	Texto que indica el tipo de suceso dentro de *Categoría*.
Estado de suceso*	Instrucciones de manejo de suceso.
Ámbito de suceso*	Público al que va dirigido el mensaje.
Restricción	Información adicional cuando *Ámbito del suceso* es "Restringido".
Titular*	Descripción breve del suceso.
Categoría*	Clasificación de sucesos de alto nivel
Gravedad*	Intensidad de la repercusión del suceso.

Tabla 87. Propiedades de suceso (continuación)

Propiedad	Contenido
Quién	
Certeza*	Confianza en la predicción del suceso.
Urgencia*	Cronograma para la acción de respuesta al suceso.
Tipo de mensaje	Naturaleza del mensaje.
Descripción	Descripción adicional del suceso.
Dirección web	Dirección web para obtener información adicional sobre el suceso.
Cuándo	
Fecha y hora de envío	Fecha y hora a las que se ha enviado o sometido el mensaje.
Fecha y hora efectivas	Fecha y hora a las que el mensaje es efectivo.
Fecha y hora de inicio	Fecha y hora en la que se espera que comience el suceso
Fecha y hora de caducidad	Fecha y hora a las que se espera que finalice el suceso.
Dónde	
Descripción de área	Descripción del área afectada.
Latitud/longitud	Coordenadas de la ubicación del suceso.

Nota: Las propiedades marcadas con un asterisco en la tabla son necesarias para la correcta creación de un nuevo suceso. Las propiedades que no están marcados con un asterisco son opcionales cuando al crear un suceso.

Gestión de sucesos e incidencias

En el portlet de Detalles, puede realizar varias acciones sobre los suceso que aparecen en la lista de la pestaña **Sucesos e incidencias**. En el portlet Mapa, puede agregar un suceso que se muestra tanto en el mapa como en la lista de sucesos del portlet Detalles.

Procedimiento

En la pestaña **Sucesos e incidencias**, pulse el botón derecho del ratón en una fila de la lista de sucesos y seleccione una opción del menú:

- Para actualizar la información sobre un suceso, pulse **Actualizar suceso**. Puede especificar los cambios en una ventana con campos que contienen información sobre el suceso. Cuando un registro de sucesos se actualiza, la propiedad de tipo de mensaje cambia a *Actualizar*.
- Para cambiar el estado de un suceso a incidencia, pulse **Escalar a incidencia** para mostrar una ventana y especificar los detalles de contacto. Cuando se escala un registro de sucesos, se produce un cambio en las propiedades y en el icono del mapa.
- Para eliminar un suceso de la lista y el mapa, pulse **Cancelar suceso** para mostrar una ventana y especificar sus datos de contacto.
- Para ver el procedimiento operativo estándar (SOP) y las actividades de flujo de trabajo asociadas con un suceso, pulse **Ver detalles del procedimiento operativo estándar**. Si no hay procedimientos de operación estándar asociados con un suceso, esta opción no está disponible. Si hay un procedimiento operativo estándar asociado, se mostrará la ventan Información de funcionamiento estándar del procedimiento. Utilice el portlet Mis actividades para gestionar las actividades de flujo de trabajo asociadas con un procedimiento operativo estándar.
- Para ver una lista de los recursos en las proximidades de un suceso, pulse **Ver recursos cercanos** y seleccione el radio de la zona en la que desea centrarse. Se muestra una lista de recursos en la pestaña **Recursos**.

- Para ver la información acerca de un sucesos, pulse **Propiedades** para mostrar la ventana que contiene campos con información acerca del suceso.

Gestión de recursos

Puede realizar varias acciones en los recursos de la lista en la pestaña **Recursos** .

Procedimiento

En la pestaña **Recursos** , pulse con el botón derecho del ratón sobre una fila de la lista de recursos y seleccione una opción del menú:

- Para actualizar la información sobre un recurso, haga clic en **Actualizar**.
- Para eliminar un recurso de la lista y el mapa, pulse **Suprimir**.
- Para ver la información acerca de un recurso, pulse **Propiedades**.

Cualquiera que sea la opción que elige, se muestra el recurso en Tivoli Service Request Manager, en la pestaña **Recursos** . También puede ver las prestaciones para el recurso en la pestaña Tivoli Service Request Manager **Prestaciones** . Para actualizar o suprimir un recurso, seleccione el recurso y, a continuación, seleccione la opción adecuada desde la lista **Seleccionar acción** .

Personalización del portlet Detalles

Administrador

Si tiene acceso de administrador, puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Establezca los parámetros para el portlet Detalles de la siguiente manera:

Mediante la definición de parámetros para el portlet Detalles, puede hacerse lo siguiente:

- Especifique la disposición de las columnas, los encabezados, el orden de clasificación y la prioridad.
- Especifique las condiciones adicionales para filtrar los sucesos o recursos que se muestran.
- Mostrar u ocultar el
  - botón **Añadir suceso**
  - botón **Añadir recurso**
  - pestaña **Sucesos**
  - pestaña **Recursos**
  - barra de herramientas en la parte superior de la lista.
- Especifique un nombre de grupo que permita la comunicación con otros portlets de mapa y Detalles.
- Defina el portlet para que reconozca o ignore tipos específicos de mensajes que proceden de otros portlets del grupo.

Puede definir parámetros de portlet genéricos que sean comunes a todos los portlets: ubicación del archivo de ayuda, altura del portlet, título del portlet y paquete de recursos.

Referencia relacionada:

"Valores del portlet Detalles" en la página 152
Personalice el portlet Detalles cambiando los valores en los campos de la ventana **Valores compartidos** .

Obtención de detalles de indicador clave de rendimiento

Utilice el portlet Obtención de detalles de indicador clave de rendimiento para ver información adicional acerca de una categoría de ICR, el estado de sus ICR subyacentes.

El portlet Obtención de detalles de indicador clave de rendimiento muestra todos los ICR subyacentes asociados con una categoría de organización o de ICR que se muestra en el portlet Estado. Los ICR se muestran en forma de una lista anidada que se puede expandir o contraer. El estado de cada ICR subyacente está representado por el color, de la misma manera que se utiliza el color para las categorías de ICR mostradas en el portlet Estado. Los valores de los ICR subyacentes controlan el color del ICR primario. Para mostrar el estado del ICR, desplace el cursor sobre dicho ICR.

Para centrarse en un categoría de ICR específica en el portlet Obtención de detalles de indicador clave de rendimiento, haga clic en la categoría en el portlet Estado. Luego esta categoría se muestra en solitario en el portlet Obtención de detalles de indicador clave de rendimiento. Puede utilizar la lista para inspeccionar los ICR subyacentes hasta llegar a los detalles del ICR que causara el cambio de estado.

Administrador

Personalización del portlet Obtención de detalles de indicador clave de rendimiento

Si tiene acceso de administrador, puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Mediante la definición de parámetros para el portlet Obtención de detalles de indicador clave de rendimiento, puede hacerse lo siguiente:

- Especifique la disposición de las columnas, los encabezados, el orden de clasificación y la prioridad.
- Personalizar los colores de ICR.
- Habilitar un filtro de ICR adicional.
- Muestre u oculte la barra de herramientas en la parte superior de la lista.
- Especifique un nombre de grupo para permitir la comunicación con un portlet Obtención de detalles de indicador clave de rendimiento.

Puede definir parámetros de portlet genéricos que sean comunes a todos los portlets: ubicación del archivo de ayuda, altura del portlet, título del portlet y paquete de recursos.

Conceptos relacionados:

"Indicadores clave de rendimiento" en la página 173
Utilice el portlet Indicadores clave de rendimiento para personalizar los indicadores clave de rendimiento (ICR) y su visualización jerárquica en IBM Intelligent Operations Center.

Referencia relacionada:

"Valores del portlet Obtención de detalles de indicador clave de rendimiento" en la página 156
Personalice el portlet Obtención de detalles de indicador clave de rendimiento cambiando los valores en los campos de la ventana **Valores compartidos** .

Mapa de ubicación

Utilice el Mapa de ubicación portlet para ver los sucesos marcados en un mapa de ubicación. Un mapa de ubicación en IBM Intelligent Operations Center es un mapa o plano con zonas predefinidas para la interacción, por ejemplo, los asientos en un estadio deportivo.

El portlet Mapa de ubicación le proporciona una representación visual de los sucesos en la posición en la que se producen. El portlet Mapa de ubicación, junto con los portlets Mapa y Detalles, permiten identificar problemas, patrones de ubicación, conflictos y sinergias.

Los portlets Mapa de ubicación, Mapa y Detalles se pueden enlazar para compartir entradas y cambios en los sucesos que se muestran. Puede seleccionar las categorías de sucesos que desea ver en el portlet Mapa de ubicación . La selección afecta a los sucesos visualizados en el portlet Mapa de ubicación y en los portletsMapa y Detalles a los que está vinculado.

Interfaz de Mapa de ubicación

El portlet Mapa de ubicación cuenta con tres elementos de interfaz interactivos, como se muestra en la siguiente tabla:

Tabla 88. Elementos de interfaz del portlet Mapa de ubicación

Elemento de la interfaz	Descripción
Mapa de ubicación	Un diagrama de la ubicación con marcadores para sucesos.
Seleccionar contenido: categorías de suceso	Un formulario de filtro para seleccionar las categorías de los sucesos que se muestran en el mapa.
Menú Mapa	Una lista de los mapas de ubicación disponibles organizados por clasificación.

Inicialmente, la página del portal se abre con el portlet Mapa de ubicación y todos los sucesos que le son relevantes mostrados en el mapa de ubicación. El mapa se actualiza con los nuevos sucesos, sujetos a los filtros que establece para limitar las categorías mostradas.A la izquierda del mapa se proporciona una barra de menú con todos los mapas disponibles.

Se ha producido un suceso que está representado por un marcador en una posición concreta en el mapa de ubicación. Puede visualizar el título y la descripción de un suceso desplazando el ratón sobre el marcador de suceso en el mapa. La ventana incluye el nombre y la descripción del área en la que se produce el suceso. Si se produce más de un suceso en la misma área, los sucesos se agrupan y se representan mediante un marcador de clúster. Al pasar el ratón por encima de este marcador, el titular de cada suceso se incluye en la ventana. También puede ver el nombre y descripción de la zona pasando el cursor sobre cualquiera de las áreas predefinidas del mapa que no tienen sucesos.

Donde se unen los portlets, puede pulsar un marcado de este portlet y también se seleccionan los sucesos correspondientes en otros portlets del grupo. Igualmente, seleccionando un suceso en cualquiera de los portlets vinculados da como resultado que ese suceso destaque en este portlet.

Nota: Un suceso debe tener un identificador de área que se visualizará en el portlet Mapa de ubicación . Además, un suceso debe tener coordenadas de latitud y longitud que se mostrarán en los portlets Mapa de ubicación y Mapa . Si un suceso no tiene identificador de área o coordenadas, se puede visualizar únicamente en el portlet Detalles .

Marcadores de mapa

El mapa representa la ubicación de sucesos con uno de los siguientes tipos de marcador:

Tabla 89. Marcadores de mapa

Tipo de marcador	Descripción
Icono	Señala en el mapa la posición de un suceso mediante un icono exclusivo para cada tipo de categoría de suceso.
Clúster	Indica más de un suceso en la misma área, con un número que representa el número de sucesos en esa área.

El icono que representa un tipo de suceso se define en el campo de categoría de los detalles del suceso en la pestaña **Sucesos e incidencias** del portlet Detalles. Cuando un suceso se escala a incidencia, el icono

que aparece en el mapa conserva su símbolo específico de categoría, con el añadido de un margen rojo alrededor del icono.

Controles del mapa

Puede desplazarse por el mapa con el ratón o el teclado.

Los controles del mapa están en el lado superior izquierdo del mapa.

Los controles del mapa se encuentran en el lado superior izquierdo del mapa. Se componen de:

- Flechas de dirección (arriba, abajo, izquierda, derecha)
- Acercar
- Vista global (se aleja hasta el máximo)
- Zoom para alejar

Controles de dirección para desplazarse por el mapa

Para desplazarse por el mapa, puede:

- Pulsar y arrastrar el mapa con el ratón
- Pulsar la flecha de dirección hacia arriba o la tecla de fecha hacia arriba del teclado para desplazarse hacia el norte
- Pulsar la flecha de dirección hacia abajo o la tecla de fecha hacia abajo del teclado para desplazarse hacia el sur
- Pulsar la flecha de dirección hacia la derecha o la tecla de fecha hacia la derecha del teclado para desplazarse hacia el este
- Pulsar la flecha de dirección hacia la izquierda o la tecla de fecha hacia la izquierda del teclado para desplazarse hacia el oeste

Controles de zoom para ampliar o reducir la escala del mapa

Para acercar y alejar el mapa, puede:

- Pulsar el icono de mapa **+** para acercar la imagen, o el icono de mapa **-** para alejarla del centro del mapa
- Efectuar una doble pulsación para centrar el mapa y ampliar la ubicación seleccionada
- Pulsar el icono **Vista global** para alejar la imagen al máximo y mostrar una vista general
- Pulsar la tecla **+** del teclado para acercar la imagen
- Pulsar la tecla **-** del teclado para alejar la imagen
- Pulsar la tecla Mayús mientras pulsa el ratón para dibujar un rectángulo alrededor del área para ampliarla

Selección de categorías de sucesos para el mapa

Con el filtro Categorías de suceso, puede seleccionar por categoría qué sucesos se muestran en el mapa.

Para ver el formulario de filtro, pulse **Seleccionar contenido**. Las categorías de suceso visualizadas en el mapa y en los portlets asociados, pueden cambiar en base a la selección del formulario de filtro que se haya aquí. Puede centrarse en las categorías de suceso que desee analizar mediante el uso del filtro para ocultar las categorías de sucesos que no necesite. El mapa responde a cualquier cambio en el formulario de filtro. Cuando se cambia la selección, el mapa se actualiza y en el mapa solo se trazan las posiciones de los sucesos dentro de las categorías seleccionadas. Cambie las categorías de suceso mostradas seleccionando o borrando las casillas de verificación del formulario de filtro. Para cerrar el formulario de filtro, pulse **Seleccionar contenido**. Si deja la página del portal y vuelve, el filtro se establece a la selección predeterminada.

Puede centrarse en sucesos individuales que desea analizar seleccionando las casillas de verificación en el portlet Detalles . Luego estos suceso se resaltan también en los portlets enlazados.

Personalización del portlet Mapa de ubicación

Administrador

Si tiene acceso de administrador, puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Los portlets Mapa yMapa de ubicación también se pueden personalizar cambiando los valores globales. Los valores globales afectan al contenido de este portlet para todos los usuarios y para todas las apariciones del portlet. Los valores globales son reemplazados por los valores compartidos.

Los valores que cambia para el portlet Mapa de ubicación son los siguientes:

- La selección predeterminada en el filtro de Categorías de suceso.
- El nombre del mapa de ubicación predeterminado que se va a mostrar.
- El color predeterminado para resaltar el área, cuando se utiliza el cursor para desplazarse sobre un área.
- El nombre del grupo que permite la comunicación con otro mapa y portlets Detalles.

Puede definir parámetros de portlet genéricos que sean comunes a todos los portlets: ubicación del archivo de ayuda, altura del portlet, título del portlet y paquete de recursos.

Personalización de mapas de ubicación

Puede utilizar el portlet Gestor de mapas de ubicación para personalizar los siguientes aspectos del portlet Mapa de ubicación.

- Nombre de clasificación que se va a mostrara en el menú a la izquierda del portlet.
- El mapa que se visualizará en el portlet.
- Áreas dentro de un mapa.

Conceptos relacionados:

"Gestor de mapas de ubicación" en la página 181
Utilice el portlet Gestor de mapas de ubicación para personalizar el portletMapa de ubicación .

Referencia relacionada:

"Valores del portlet Mapa de ubicación" en la página 159
Personalice el portlet Mapa de ubicación cambiando los valores en los campos de la ventana **Valores compartidos** .

Mapa

Uso del portlet Mapa para ver sucesos y recursos en un mapa.

El portlet Mapa le proporciona una representación visual de sucesos y recursos en un mapa. Use el portlet Mapa junto con los portlets Mapa de ubicación y Detalles , para identificar patrones de ubicación, conflictos, problemas y sinergias.

Los portlets Mapa, Mapa de ubicación y Detalles se pueden unir para compartir la entrada y los cambios a los sucesos mostrados. En el portlet Mapa , puede seleccionar las categorías de sucesos y las prestaciones de recursos que desea visualizar. La selección afecta a lo que se muestra en el portletMapa y en los portlets Mapa de ubicación y Detalles vinculados.

Interfaz de mapa

El portlet Mapa cuenta con tres elementos de interfaz interactivos, como se muestra en la siguiente tabla:

Tabla 90. Elementos de interfaz del portlet Mapa

Elemento de la interfaz	Descripción
Mapa	Un mapa de la región geográfica con marcadores de sucesos y recursos.
Seleccionar contenido: categorías de suceso	Un formulario de filtro para seleccionar las categorías de los sucesos que se muestran en el mapa y en los portlets enlazados con el portlet Mapa.
Seleccionar contenido: recursos	Un formulario de filtro para seleccionar las prestaciones de los recurso que se muestran en el mapa y en la pestaña **Recursos**, en el portlet Detalles enlazado. Para ver este formulario, seleccione primero **Ver recursos de la zona** en el portlet Detalles .

Inicialmente, la página de portal se abre con el portlet Mapa y con todos los sucesos que son relevantes para el usuario en el mapa. Si un suceso tiene valores de latitud y longitud especificados, puede ver la ubicación de suceso en forma de marcador de icono en el mapa. Puede visualizar el título y la descripción de un suceso desplazando el ratón sobre el marcador de suceso en el mapa. Si hay más de un suceso agrupado en clústeres en la misma ubicación, se indica el número de sucesos en el marcador. Al pasar el ratón por encima del marcador de clústeres, el titular de cada suceso se incluye en la ventana. El mapa se actualiza con los nuevos sucesos, sujetos a los filtros que establece para limitar las categorías mostradas.

Donde se unen los portlets, puede pulsar un marcador de suceso en un portlet y también se selecciona el suceso correspondiente en los demás portlets del grupo.

Existe un límite para el número de marcadores que se puede mostrar en el mapa. Si el número de marcadores en el área de la vista supera el umbral, los marcadores no se muestran. Se recibe un mensaje con el número de marcadores disponibles y el número del umbral. Se ofrecen dos opciones para visualizar todos los marcadores disponibles:

- Acerque o enfoque un área del mapa con el número de marcadores por debajo del umbral.
- Pulse **Cargar todos los elementos en la vista**.

Si elige la segunda opción, puede observar que los marcadores aparecen en el mapa a un ritmo más lento. Hay una tercera opción: utilice el filtro para seleccionar menos categorías.

Si se selecciona **Ver recursos cercanos** para un suceso en el portlet Detalles, los recursos se muestran en el mapa basado en base al radio y las prestaciones que se han seleccionado.

El mapa mantiene al usuario actualizado añadiendo nuevos sucesos, sujetos a los filtros definidos para limitar las categorías que se muestran.

Nota: Si un suceso tiene un identificador de área además de las coordenadas de latitud y longitud, se puede visualizar en los portlets Mapa de ubicación y Mapa . Todos los sucesos se pueden visualizar en el portlet Detalles .

Marcadores de mapa

El mapa representa la ubicación de sucesos o recursos con uno de los siguientes tipos de marcador:

Tabla 91. Marcadores de mapa

Tipo de marcador	Descripción
Icono	Puntos en el mapa que marcan la posición de un suceso o recursos con un único icono para cada tipo de recurso o categoría.

Tabla 91. Marcadores de mapa (continuación)

Tipo de marcador	Descripción
Polígono	traza en el mapa el área asociado con un suceso concreto
Clúster	indica más de un suceso en la misma zona con un número que representa el número de sucesos de esa zona.
Radio	Delinea en el mapa el área que seleccione para **Ver recursos cercanos** en relación con un suceso.

El icono que representa un tipo de suceso se define en el campo de categoría de los detalles del suceso en la pestaña **Sucesos e incidencias** del portlet Detalles. Cuando un suceso se escala a incidencia, el icono que aparece en el mapa conserva su símbolo específico de categoría, con el añadido de un margen rojo. Al pulsar un marcador de suceso en el mapa, se resalta el suceso o los sucesos asociados en el portlet Detalles.

El icono que representa a un recurso se define en el campo de tipo de los detalles del recurso en la pestaña **Recursos** del portlet Detalles . Para ver iconos de recurso, seleccione en primer lugar **Ver recursos cercanos** en el portlet Detalles.

Uso de los controles del mapa

Puede desplazarse por el mapa con el ratón o el teclado.

Los controles del mapa están en el lado superior izquierdo del mapa.

Los controles del mapa se encuentran en el lado superior izquierdo del mapa. Se componen de:

- Flechas de dirección (arriba, abajo, izquierda, derecha)
- Acercar
- Vista global (se aleja hasta el máximo)
- Zoom para alejar

Controles de dirección para desplazarse por el mapa

Para desplazarse por el mapa, puede:

- Pulsar y arrastrar el mapa con el ratón
- Pulsar la flecha de dirección hacia arriba o la tecla de fecha hacia arriba del teclado para desplazarse hacia el norte
- Pulsar la flecha de dirección hacia abajo o la tecla de fecha hacia abajo del teclado para desplazarse hacia el sur
- Pulsar la flecha de dirección hacia la derecha o la tecla de fecha hacia la derecha del teclado para desplazarse hacia el este
- Pulsar la flecha de dirección hacia la izquierda o la tecla de fecha hacia la izquierda del teclado para desplazarse hacia el oeste

Controles de zoom para ampliar o reducir la escala del mapa

Para acercar y alejar el mapa, puede:

- Pulsar el icono de mapa **+** para acercar la imagen, o el icono de mapa **-** para alejarla del centro del mapa
- Efectuar una doble pulsación para centrar el mapa y ampliar la ubicación seleccionada
- Pulsar el icono **Vista global** para alejar la imagen al máximo y mostrar una vista general
- Pulsar la tecla **+** del teclado para acercar la imagen

- Pulsar la tecla **-** del teclado para alejar la imagen
- Pulsar la tecla Mayús mientras pulsa el ratón para dibujar un rectángulo alrededor del área para ampliarla

Selección de categorías de sucesos para el mapa

Utilice el filtro Categorías de suceso para seleccionar por categoría qué sucesos se muestran en el mapa.

Para ver el formulario de filtro, pulse **Seleccionar contenido**. Las categorías de sucesos visualizadas en el portlet del mapa se puede cambiar en base a la selección de formulario de filtro que hace. Puede centrarse en las categorías de suceso que desee analizar mediante el uso del filtro para ocultar las categorías de sucesos que no necesite. El mapa responde a cualquier cambio en el formulario de filtro. Un cambio en el formulario de filtro también afecta a otros portlets del mismo grupo. Cuando se cambia una selección, el mapa se actualiza y en el mapa solo se trazan las ubicaciones de los sucesos dentro de las categorías seleccionadas. Cambie las categorías de suceso mostradas seleccionando o borrando las casillas de verificación del formulario de filtro. Para cerrar el formulario de filtro, pulse **Seleccionar contenido**. Si sale de la página de portal y vuelve, el filtro se restablece al valor predeterminado, que es todas las categorías seleccionadas.

Puede centrarse en sucesos individuales que desee analizar marcando casillas de verificación en el portlet Detalles. Estos sucesos se resaltan en el mapa.

Selección de las prestaciones de recursos para el mapa

Si se selecciona **Ver recursos cercanos** en el portlet Detalles, el filtro Categorías de suceso se sustituye por el filtro Recursos. Utilice el filtro Recursos para seleccionar por capacidad los recursos que se muestran en el mapa.

Para ver el formulario de filtro, pulse **Seleccionar contenido**. Las prestaciones de recursos que aparecen en el mapa y en el portlet Detalles se pueden cambiar en base a la selección del formulario de filtro que se realice. Puede centrarse en la prestación que desee analizar mediante el uso del filtro para ocultar las prestaciones que no necesite. El mapa responde a cualquier cambio en el formulario de filtro. Un cambio en el formulario de filtro también afecta al portlet Detalles del mismo grupo. Cuando se cambia una selección, el mapa se actualiza y en el mapa solo se trazan las ubicaciones de los recursos con las prestaciones seleccionadas. Cambie la prestación de recurso mostrada seleccionando o borrando una casilla de verificación del formulario de filtro. Para cerrar el formulario de filtro, pulse **Seleccionar contenido**. Si sale de la página de portal y vuelve al formulario de filtro de recursos, el filtro se restablece al valor predeterminado, que es todas las prestaciones seleccionadas. Las prestaciones seleccionadas de forma predeterminada dependen de la categoría del suceso y de cómo esa categoría está correlacionada con prestaciones.

Restablecimiento del mapa

El portlet Mapa se puede restablecer a la vista predeterminada configurada para IBM Intelligent Operations Center.

Procedimiento

1. En el portlet Mapa, haga clic en **Restablecer el mapa** o haga clic en la flecha de la esquina superior derecha.
2. Seleccione una de las opciones siguientes:
   - **Restablecer el mapa** para hacer zoom y centrar el mapa en el valor predeterminado.
   - **Restablecer el mapa y eliminar filtros** para hacer zoom y centrar el mapa en la configuración predeterminada y restablecer los valores establecidos en **Seleccionar contenido** a los valores predeterminados.

Resultados

El mapa se restablece de acuerdo con la opción seleccionada, pero sólo para la vista y el usuario actual.

Añadir un suceso

Puede crear un suceso agregándolo al mapa del portlet Mapa y a la lista del portlet Detalles al mismo tiempo. El mapa y la lista ofrecen dos maneras de ver el mismo contenido.

Acerca de esta tarea

Utilice el cuadro de diálogo **Añadir suceso** para especificar las propiedades del suceso, como se describe en la tabla siguiente:

Tabla 92. Propiedades de suceso

Propiedad	**Contenido**
Quién	
Remitente	Origen o ID de usuario
Nombre de la persona de contacto	Persona con la que ponerse en contacto para obtener información adicional.
Correo electrónico de contacto	Dirección de correo electrónico de la persona de contacto.
Teléfono de contacto	Número de teléfono de la persona de contacto
Qué	
Tipo de suceso*	Texto que indica el tipo de suceso dentro de *Categoría*.
Estado de suceso*	Instrucciones de manejo de suceso.
Ámbito de suceso*	Público al que va dirigido el mensaje.
Restricción	Información adicional cuando *Ámbito del suceso* es "Restringido".
Titular*	Descripción breve del suceso.
Categoría*	Clasificación de sucesos de alto nivel
Gravedad*	Intensidad de la repercusión del suceso.
Certeza*	Confianza en la predicción del suceso.
Urgencia*	Cronograma para la acción de respuesta al suceso.
Tipo de mensaje	Naturaleza del mensaje.
Descripción	Descripción adicional del suceso.
Dirección web	Dirección web para obtener información adicional sobre el suceso.
Cuándo	
Fecha y hora de envío	Fecha y hora a las que se ha enviado o sometido el mensaje.
Fecha y hora efectivas	Fecha y hora a las que el mensaje es efectivo.
Fecha y hora de inicio	Fecha y hora en la que se espera que comience el suceso
Fecha y hora de caducidad	Fecha y hora a las que se espera que finalice el suceso.
Dónde	
Descripción de área	Descripción del área afectada.
Latitud/longitud	Coordenadas de la ubicación del suceso.

Procedimiento

1. Pulse con el botón derecho del ratón sobre una ubicación en el mapa y pulse **Añadir suceso** para iniciar el cuadro de diálogo **Añadir suceso** . Algunas de las propiedades de suceso se completan de forma automática.
2. Especifique las propiedades de suceso restantes en los campos del diálogo. Las propiedades marcadas con un asterisco son necesarias para la correcta creación de un suceso nuevo. Las propiedades no marcadas con un asterisco son opcionales.
3. Pulse **Aceptar** para guardar el suceso o en **Cancelar** para dejar de añadir el suceso.

Resultados

Se muestra un icono que representa la categoría de un suceso nuevo en la ubicación solicitada en el mapa. Puede ver los detalles del nuevo suceso en la lista de portlet Detalles vinculada.

Personalización del portlet Mapa

Administrador

Si tiene acceso de administrador, puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Los portlets Mapa yMapa de ubicación también se pueden personalizar cambiando los valores globales. Los valores globales afectan al contenido de este portlet para todos los usuarios y para todas las apariciones del portlet. Los valores globales son reemplazados por los valores compartidos.

Puede cambiar los siguientes valores específicos para el portlet Mapa :

- Restablezca el punto central predeterminado y el nivel de zoom para el mapa.
- Seleccione un nuevo mapa de base. El valor predeterminado es un mapa de ArcGIS suministrado por Esri.
- Añada la anotación geográfica del mapa y las capas de visualización en KML (Keyhole Markup Language), para representar datos adicionales.
- Establezca el umbral para el número de marcadores que puede visualizan sin un mensaje de aviso.
- Defina la selección por defecto en los filtros del mapa, que se muestra al pulsar **Seleccionar contenido**.
- Especifique el nombre del grupo que permite la comunicación con otro mapa y portlets Detalles.

Puede definir parámetros de portlet genéricos que sean comunes a todos los portlets: ubicación del archivo de ayuda, altura del portlet, título del portlet y paquete de recursos.

Referencia relacionada:

"Valores del portlet Mapa" en la página 161
Personalice el portlet Mapa cambiando los valores en los campos de la ventana **Valores compartidos** .

Mis actividades

El portlet Mis actividades muestra una lista dinámica de actividades que son propiedad del grupo del que es miembro el usuario que tiene sesión iniciada en la interfaz.

Cada vez que un suceso desencadena un procedimiento operativo estándar de acuerdo con los criterios de selección definidos en matriz de selección del procedimiento de operación estándar, las actividades asociadas se asignan a los propietarios. Para obtener más información sobre los procedimientos de operación estándar, consulte el enlace que aparece al final del tema

Un usuario que haya iniciado sesión puede ver las actividades asignadas a ellos en el portlet Mis actividades. En el portlet Mis actividades, las actividades se agrupan por sus procedimientos de operación estándar de nivel superior. Cada procedimiento operativo estándar se corresponde con un suceso individual.

Para cada procedimiento operativo estándar, el portlet Mis actividades solo visualiza actividades abiertas y actividades no cerradas o completadas. Las actividades abiertas son aquellas actividades que ya están iniciadas y las actividades que son elegibles para ser iniciadas. Por ejemplo, si una o más de las actividades que se especifican en un procedimiento operativo estándar están ordenados en una secuencia, sólo se visualiza la actividad actual de la secuencia. Si una actividad en particular se basa en la finalización de una actividad anterior, dicha actividad no se muestra hasta que la actividad anterior se haya completado o se haya saltado.

Los siguientes iconos de vencimiento de actividad se muestran cerca de la parte superior del portlet Mis actividades:

Vencida
Actividades cuya terminación está retrasada.

Hoy Actividades que se deben completar hoy.

Futuro
Actividades cuya terminación vence en el futuro.

Cuando se inicia una actividad, la fecha de vencimiento se calcula sumando la hora de inicio a la duración de la actividad. Las fechas de vencimiento de actividad se utilizan para calcular el número que aparece en cada uno de los iconos de vencimiento de actividad.

En el portlet Mis actividades, los procedimientos de operación estándar que tienen actividades retrasadas se visualizan primero y los restantes procedimientos de operación estándar se visualizan en orden alfabético.

Al lado de cada procedimiento operativo estándar de la lista que tiene actividades retrasadas, un icono rojo indica el número de actividades que están retrasadas. Los procedimientos de operación estándar con actividades retrasadas se ordenan en función del número de actividades pasadas que contienen. El procedimiento operativo estándar que tiene las actividades más retrasadas se muestra en la parte superior de la lista.

Gestión de actividades en el portlet Mis actividades

Gestione sus actividades en el portlet Mis actividades:

- Para ver detalles acerca de un procedimiento operativo estándar, expanda el nombre de dicho procedimiento operativo estándar.
  - Se muestra el nombre del suceso que desencadenó el procedimiento operativo estándar. Desplace el ratón sobre el nombre del suceso para ver información de ayuda contextual que incluye la fecha y la hora de inicio del suceso y la categoría, la gravedad, la certeza y la urgencia del suceso.
  - Si el portlet Detalles se muestra en la página, para ver las propiedades del suceso haga clic en su nombre. Se visualiza la ventana Propiedades.
  - Se muestran los pasos que están en curso o que no son elegibles iniciarse. Además, también se visualizan el estado y la fecha de vencimiento de cada paso.
- Para ver más detalles sobre un paso, incluidos los comentarios y las referencias que los usuarios han añadido al paso, expanda el nombre del paso.
- Para iniciar, terminar, o saltarse un paso, expanda el nombre de este y luego elija una de las siguientes opciones:
  - Para iniciar un paso de la lista, seleccione **Iniciar**. Si el paso está definido como una tarea automática en el procedimiento operativo estándar, el flujo de trabajo asignado a la tarea se inicia

automáticamente y el paso finaliza automáticamente. El usuario que se inicia un paso se convierte en el propietario de ese paso, y el nombre del usuario se muestra en el campo **Propietario**.

- Para saltarse un paso de la lista, seleccione **Saltar**.
- Para finalizar un paso de la lista, seleccione **Finalizar**.

- Para añadir un comentario a un paso, utilice los siguientes subpasos:
  1. Expanda el nombre del paso.
  2. En la lista, seleccione **Añadir comentario**.
  3. En la ventana Añadir comentario, escriba un comentario en el campo **Comentario**. Los campos **Nombre del comentarista** y **Nombre de actividad** son de sólo lectura y contienen valores escritos automáticamente.
  4. Pulse **Aceptar**.
  5. Vuelva a expandir el nombre del paso. El nuevo comentario se visualiza al final de la lista de comentarios y referencias existentes para el paso.
- Para añadir una referencia a un paso, utilice los siguientes subpasos:
  1. Expanda el nombre del paso.
  2. En la lista, seleccione **Añadir referencia**.
  3. En la ventana Añadir referencia, escriba valores para **Nombre de referencia** y **URI de referencia**. El campo **Nombre de actividad** es de sólo lectura y contiene un valor que se escribe automáticamente.
  4. Pulse **Aceptar**.
  5. Vuelva a expandir el nombre del paso. La nueva referencia se visualiza como un enlace al final de la lista de comentarios y referencias existentes para el paso.
- Para ver los detalles correspondientes a un procedimiento operativo estándar, haga clic en el icono **i** situado junto al nombre del procedimiento operativo estándar. En la ventana Detalles de procedimiento operativo estándar se visualizan todos los pasos de actividad que se incluyen en el procedimiento operativo estándar, incluidos aquellos pasos que están en curso, son elegibles para iniciarse, se han completado y están cerrados. También se visualizan el estado y la fecha de vencimiento de cada paso. Para ver más detalles acerca de un paso, expanda su nombre.

Administrador

Personalización del portlet Mis actividades

Si tiene acceso de administrador, puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Para el portlet Mis actividades, puede especificar un nombre de grupo para permitir la comunicación con otros portlets; por ejemplo, los portlets Detalles.

Puede definir parámetros de portlet genéricos que sean comunes a todos los portlets: ubicación del archivo de ayuda, altura del portlet, título del portlet y paquete de recursos.

Conceptos relacionados:

"Procedimientos operativos estándar" en la página 131
Puede definir procedimientos de operación estándar y actividades para gestionar sucesos que vienen con IBM Intelligent Operations Center. Utilice el portlet Procedimientos operativos estándar para acceder a las aplicaciones procedimiento operativo estándar, matriz de selección del procedimiento de operación estándar y diseñador del flujo de trabajo en Tivoli Service Request Manager.

Referencia relacionada:

"Valores del portlet Mis actividades" en la página 163
Personalice el portlet Mis actividades cambiando los valores en los campos de la ventana **Valores compartidos** .

Notificaciones

Utilice el portlet Notificaciones para ver sus mensajes de alerta y sus detalles.

El portlet Notificaciones es una ventana interactiva que contiene una lista de todas las alertas actuales relevantes para el usuario. Sólo verá las alertas que se envíen a los grupos de usuarios de los que es miembro. Las alertas son notificaciones que se han recibido cuando:

- Varios sucesos suceden en la misma zona y en un momento similar, por lo que podrían estar en conflicto o que requerir coordinación.
- Se produce un cambio en un indicador clave de rendimiento (ICR) predefinido, si el administrador ha definido ese cambio como un desencadenante de alerta.

También puede utilizar el portlet para visualizar más detalles de una de alerta.

Lista de Notificaciones

El portlet Notificaciones proporciona una lista dinámica e interactiva de las alertas que resultan de cambios en ICR y sucesos relacionados. El papel de este portlet es llamar la atención sobre los cambios en ICR o en estado de sucesos. La lista contiene detalles clave de cada una de las alertas.

Para mostrar una descripción más detallada de una alerta, desplace el cursor sobre la fila. Para ver toda la información asociada con esa alerta en una ventana, haga clic en la fila y seleccione **Propiedades**.

Inicialmente, cuando se abre la página de portal, el portlet muestra todas las alertas actuales. Elimine cualquier alerta desde el portlet pulsando el botón derecho en la fila y seleccione **Cerrar alerta**. Es posible cerrar varias alertas de esta manera si se seleccionan varias filas. Cierre una alerta únicamente después de haberla gestionado adecuadamente, ya que la alerta se elimina para todos los destinatarios cuando la cierre.

Haga clic en el botón de la esquina superior derecha de la ventana para cancelarla y volver a la lista.

Un contador en la esquina izquierda de la barra de acciones al final de la lista indica el número de elementos visualizados y el número total de elementos. En el centro de la barra de acciones, puede seleccionar el número de elementos que se visualizarán al mismo tiempo. Si hay más filas que se pueden visualizar a la vez, puede desplazarse hacia adelante o hacia atrás haciendo clic en los botones de la esquina derecha de la barra de acciones.

Propiedades de alerta

La ventana de detalles de la alerta visualiza las siguientes propiedades:

Tabla 93. Propiedades de alerta

Propiedad	Contenido
Título	Descripción breve de la alerta

Tabla 93. Propiedades de alerta (continuación)

Propiedad	Contenido
Categoría	Clasificación de alto nivel del suceso o ICR
Remitente	Origen de la alerta
Enviada a grupos	Grupos a los que se ha enviado la alerta.
Enviada	Fecha y hora a las que se ha enviado la alerta.
Descripción	Descripción adicional de la alerta
Se refiere a alertas	Identificador de suceso, si la alerta ha sido causada por sucesos correlacionados
Se refiere a ICR	Nombre del ICR, si la alerta se debe al cambio de valor de un ICR

Administrador

Personalización del portlet Notificaciones

Si tiene acceso de administrador, puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Mediante la definición de parámetros para el portlet Notificaciones, puede hacerse lo siguiente:

- Especifique la disposición de las columnas, los encabezados, el orden de clasificación y la prioridad.
- Muestre u oculte la barra de herramientas en la parte superior de la lista.

Puede definir parámetros de portlet genéricos que sean comunes a todos los portlets: ubicación del archivo de ayuda, altura del portlet, título del portlet y paquete de recursos.

Referencia relacionada:

"Valores del portlet Notificaciones" en la página 164
Personalice el portlet Notificaciones cambiando los valores en los campos de la ventana **Valores compartidos** .

Informes

Utilice el portlet Informes para ver un informe de sucesos como gráfico. El portlet proporciona varias opciones para agrupar suceso y puede elegir sucesos por un rango de fechas o por una fecha concreta. Estos informes le ayudan a planificar respuestas para sucesos actuales o futuros.

Creación de informes

Usted puede crear un informe personalizado para sucesos utilizando el portlet de informes. Primero, seleccione cómo desea agrupar sucesos. Por ejemplo, para ver todos los sucesos de una categoría en particular, seleccione **Categoría** en el campo **Agrupar por** . A continuación, en los campos **Seleccionar datos** , elija los datos específicos de la información que desea ver. También puede indicar una fecha o rango de fechas para los sucesos del informe. Pulse **Actualizar**, y el gráfico cambia para reflejar la información que solicitó.

Para recuperar el URL del nuevo informe, haga clic en **URL para este informe**.

La tabla 1 muestra las opciones por las que puede agrupar sucesos.

Tabla 94. Informe personalizado

Agrupar por	**Descripción**
Tipo de suceso	Muestra sucesos basados en tipo. Por ejemplo, el suceso podría ser un tornado que se acerca o un accidente de tráfico.
Gravedad	Muestra sucesos basados en la gravedad. Por ejemplo, es posible que los sucesos sean extremos o graves.
Certeza	Visualiza sucesos en base a la probabilidad que hay de que sucedan. Por ejemplo, si ha ocurrido un accidente de tráfico, la certeza podría ser "observado".
Urgencia	Muestra sucesos basados en lo urgentes que son. Por ejemplo, el suceso podría estar ocurriendo y describirse como "inmediato".
Categoría de sucesos	Muestra sucesos basados en la categoría de suceso. Puede ver, por ejemplo, todos los sucesos medioambientales, incendios o relacionados con el tráfico.
Tipo de mensaje	Visualiza sucesos en base a los tipos de mensaje, como actualizaciones y alertas.
Estado	Visualiza sucesos por estado. Los estados son: • Aceptable • Precaución • Tomar medida
Remitente	Visualiza sucesos por un remitente concreto. Por ejemplo, el suceso puede ser un problema de seguridad o un problema que afecta a IBM Intelligent Operations for Water.
Incidencia	Muestra sucesos basados en el tipo de incidencia. Por ejemplo, puede mostrar todos los accidentes de tráfico o toda la construcción de carreteras.
Código de manejo	Muestra sucesos por código de manejo. Por ejemplo, el código de manejo podría ser "suceso".
Nombre del remitente	Visualiza sucesos por el nombre del remitente.

La Tabla 2 muestra los datos que se pueden seleccionar para el informe.

Tabla 95. Datos de selección

Datos de selección	**Descripción**
Gravedad	Muestra sucesos basados en la gravedad. Por ejemplo, es posible que los sucesos sean extremos o graves.
Certeza	Visualiza sucesos en base a la probabilidad que hay de que sucedan. Por ejemplo, si ha ocurrido un accidente de tráfico, la certeza podría ser "observado".
Urgencia	Muestra sucesos basados en lo urgentes que son. Por ejemplo, el suceso podría estar ocurriendo y describirse como "inmediato".
Categoría de sucesos	Muestra sucesos basados en la categoría de suceso. Puede ver, por ejemplo, todos los sucesos medioambientales, incendios o relacionados con el tráfico.

Tabla 95. Datos de selección (continuación)

Datos de selección	Descripción
Tipo de suceso	Muestra sucesos basados en tipo. Por ejemplo, el suceso podría ser un tornado que se acerca o un accidente de tráfico.
Fecha de inicio	Entre la fecha para la que está visualizando sucesos. Para un rango de fechas, introduzca la fecha de inicio.
Fecha final	Entre la fecha a través de la que está visualizando sucesos.

Nota: Para que este portlet funcione como se espera, debe iniciar sesión en el portal de soluciones mediante el nombre de dominio completo del Servidor de aplicaciones de IBM Intelligent Operations Center. Si inicia sesión en el portal utilizando una dirección IP o un alias de nombre de host, en lugar del nombre de dominio completo registrado, este portlet no se mostrará correctamente.

Copia de una URL de informe

Para copiar una URL de informe y hacer que el informes se muestra en un marco en la parte derecha del portlet, pulse con botón derecho del ratón sobre la URL y seleccione **Copiar dirección de enlace**. Los términos para la opción **Copiar dirección de enlace** varía dependiendo del navegador.

Importante:
Para guardar un informe definido por el usuario y utilizar el enlace copiado aquí, introduzca la fecha de ayer en el campo **Desde la fecha** y la fecha de mañana en el campo **Hasta la fecha**. Estas fechas garantizar que obtendrá todos los datos que desea incluir en el informe definido por el usuario. Por ejemplo, para el intervalo de fechas del 8/10/2012 hasta el 8/18/2012, introduzca las siguientes fechas para los criterios de filtro:

- Desde la fecha - introducir 8/9/2012
- Hasta la fecha - introducir 8/19/2012

Ejemplos de informes

El IBM Intelligent Operations Center tiene un portlet Informes que contiene informes gráficos basados en los datos del portlet Sucesos .

El marco de informe grande es donde selecciona los parámetros para la información que aparece en el gráfico del informe.

Los dos marcos del lado derecho del portlet es donde se copian los informes definidos por el usuario.

Los informes a lo largo de la parte inferior de la página son gráficos predefinidos. Para configurar estos informes para mostrar los sucesos por fecha o rango de fechas, pulse **Configurar el informe**. Entre las fechas y pulse **Ver el informe**.

Integración de los informes

El portlet Informes proporciona un IFrame para incrustar informes o páginas de IBM Cognos Business Intelligence. Especifique la URL para el informe o página que desea integrar con el portlet.

Personalización del portlet Informes

Si tiene acceso de administrador, puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Puede establecer parámetros de portlet genéricos que son comunes entre portlets: ubicación del archivo de ayuda, altura del portlet, ancho del portlet y título del portlet . También puede especificar la URL del informe que se visualiza.

Referencia relacionada:

"Valores del portlet Informes " en la página 166
Personalice el portlet Informes cambiando los valores en los campos de la ventana **Valores compartidos** .

Estado

Utilice el portlet Estado para ver el estado de los indicadores clave de rendimiento (ICR) para una única organización o en varias organizaciones.

El portlet Estado proporciona un resumen de nivel ejecutivo del estado de los ICR en las organizaciones que tienen permiso para ver. Utilice este portlet para ver cambios actualizados en el estado de ICR para poder planificar y tomar medidas si es necesario.

Código de colores de ICR

Cada columna contiene información de ICR sobre una organización cuyo nombre aparece en la parte superior de la columna. Las categorías de ICR asociadas con cada organización se representan mediante celdas de colores. El color de fondo para una categoría de ICR refleja su estado. Si hay más de seis ICR para visualizar en una columna, el tamaño de cada célula individual se reduce para dar cabida a los ICR adicionales.

El código de colores de fondo que se proporciona con los ICR de muestra de la solución es como se indica a continuación:

- El verde indica que el estado es aceptable, en base a los parámetros para ese ICR.
- El amarillo indica que se necesita precaución o supervisión.
- El rojo indica que la acción se recomienda.
- El gris indica que no hay suficientes datos disponibles para calcular el estado del ICR.

El código de colores se define en la leyenda de la parte superior del portlet.

Un estado no determinado indica que no hay ningún valor de ICR disponible durante el periodo de tiempo definido para ese ICR. Esta situación se produce cuando la solución no recibe ningún mensaje para el ICR en el periodo de tiempo especificado. Por ejemplo, el nivel de agua para una fuente de agua se calcula a diario. Si no se recibe ningún mensaje de nivel de agua correspondiente a esa fuente de agua en un día determinado, entonces no hay datos para determinar el valor de ICR.

Para ver el nombre del ICR y una definición del estado representado por el color de un ICR, desplace el cursor sobre la celda.

Actualizaciones de ICR

Cuando un ICR subyacente cambia, el cambio se refleja en el portlet Estado. Por ejemplo, uno de los ICR de muestra que determinan el estado del ICR de calidad del agua cambia de estado de aceptable a precaución. El cambio se refleja en el portlet mediante un cambio en el color de fondo de la celda Calidad del agua de verde a amarillo. Además, el portlet Notificaciones indica que un ICR ha cambiado.

Cuando la solución recibe un mensaje relacionado con el cálculo de un ICR, hay un cambio de color instantáneo. Esta característica es una ventaja cuando la categoría de ICR es probable que reciba cambios en tiempo real, como por ejemplo retrasos en aeropuertos. No es relevante para aquellas categorías que contienen ICR históricos, como por ejemplo el control de inundaciones. Para esas categorías de ICR, se realizan mediciones regulares diarias y es poco probable que entretanto en haya un cambio repentino que afecte al estado.

Para cada ICR, se pueden ver todos los ICR subyacentes y sus detalles en el portlet Obtención de detalles de indicador clave de rendimiento que está enlazado con el portlet Estado.

Para centrarse solo en un ICR específico en el portlet Obtención de detalles de indicador clave de rendimiento, pulse en la celda del ICR en la tabla del portlet Estado. También puede hacer clic en el título de la organización propietaria (por ejemplo, "Agua") para ver todos los ICR relacionados.

Administrador

Personalización del portlet Estado

Si tiene acceso de administrador, puede personalizar este portlet. Pulse el botón de la esquina superior derecha del portlet para ver las opciones de personalización del menú de portlet. Los valores compartidos afectan al contenido de este portlet para todos los usuarios, pero únicamente para esta aparición del portlet.

Mediante la definición de parámetros para el portlet Estado, puede hacerse lo siguiente:

- Personalizar los colores de ICR.
- Habilitar un filtro de ICR adicional.
- Mostrar u ocultar la leyenda de ICR.
- Definir cómo se ordenan los ICR.
- Especifique un nombre de grupo para permitir la comunicación con un portlet Obtención de detalles de indicador clave de rendimiento.

Puede definir parámetros de portlet genéricos que sean comunes a todos los portlets: ubicación del archivo de ayuda, altura del portlet, título del portlet y paquete de recursos.

Personalización de los ICR

Con la solución se proporciona un conjunto de ICR de muestra. Estos ICR se han diseñado para brindar orientación para planificación e implementación de distintos tipos de ICR que se adecuen a su organización. Se proporcionan ejemplos para las áreas de agua, transporte y seguridad pública.

Conceptos relacionados:

“Indicadores clave de rendimiento” en la página 173
Utilice el portlet Indicadores clave de rendimiento para personalizar los indicadores clave de rendimiento (ICR) y su visualización jerárquica en IBM Intelligent Operations Center.

Referencia relacionada:

“Valores del portlet Estado” en la página 169
Personalice el portlet Estado cambiando los valores en los campos de la ventana **Valores compartidos** .

Capítulo 9. Solución de problemas y soporte

Para aislar y resolver problemas con el software IBM, puede utiliza r la información de resolución de problemas y soporte que contiene instrucciones para utilizar los recursos de determinación de problemas proporcionados con los productos IBM.

Técnicas para la resolución de problemas

El proceso de resolución de problemas es un enfoque sistemático para resolver un problema. El objetivo de la resolución de problemas es determinar por qué algo no funciona como se esperaba y cómo solucionar el problema.

El primer paso del proceso de resolución de problemas es describir el problema. Las descripciones de los problemas le ayudarán a usted y al personal de soporte de IBM a saber dónde comenzar a buscar el motivo del problema. En este paso debe plantearse algunas cuestiones básicas:

- ¿Cuáles son los síntomas del problema?
- ¿Dónde se produce el problema?
- ¿Cuándo se produce el problema?
- ¿En qué condiciones se produce el problema?
- ¿Se puede reproducir el problema?

Las respuestas a estas preguntas suelen llevar a una buena descripción del problema, lo que puede llevar, a su vez, a resolverlo.

¿Cuáles son los síntomas del problema?

Cuando se empieza a describir un problema, la pregunta más obvia es: "¿Cuál es el problema?" Esta pregunta puede parecer directa, sin embargo la puede dividir en varias preguntas más centradas que crean una imagen más descriptiva del problema. Estas preguntas incluyen:

- ¿Quién o qué informa del problema?
- ¿Cuáles son los códigos y mensajes de error?
- ¿Cómo falla el sistema? Por ejemplo, ¿es un bucle, un bloqueo, se reduce el rendimiento o el resultado es incorrecto?

¿Dónde se produce el problema?

No siempre es fácil determinar dónde se origina el problema, pero es uno de los pasos más importantes a la hora de solucionar un problema. Pueden existir muchas capas de tecnología entre los componentes de informe y los que fallan. Las redes, discos y controladores son solo algunos de los componentes que hay que tener en cuenta a la hora de investigar la causa de los problemas.

Las siguientes preguntas pueden ayudarle a centrarse en el origen del problema y aislar la capa del mismo:

- ¿El problema es específico de una plataforma o sistema operativo, o bien es común a varias plataformas o sistemas operativos?
- ¿Se soporta el entorno y la configuración actual?

Si una capa informa del problema, éste no tiene por qué tener su origen necesariamente en esa capa. Para identificar dónde se origina un problema hay que comprender el entorno en el que se encuentra. Dedique un poco de tiempo a describir completamente el entorno del problema, incluido el sistema operativo y la

versión, todo el software correspondiente y las versiones, así como la información de hardware. Confirme que está trabajando en un entorno con una configuración soportada; muchos problemas pueden rastrearse hasta niveles incompatibles de software que no están concebidos para funcionar juntos o no se han probado a fondo conjuntamente.

¿Cuándo se produce el problema?

Desarrolle una línea temporal detallada de sucesos que lleven hasta el error, especialmente en los casos de una única aparición. Puede desarrollar fácilmente una línea temporal si recorre el camino inverso: comience en el momento en que se informó del error (tan detalladamente como sea posible, incluso al milisegundo) y repase la información y las anotaciones disponibles hasta llegar al origen. Por lo general, sólo suele ser necesario llegar hasta el primer suceso sospechoso que encuentra en un registro de diagnóstico.

Para desarrollar una escala de tiempo detallada de sucesos, responda a estas preguntas:

- ¿El problema solo se produce a una determinada hora del día o de la noche?
- ¿Con qué frecuencia se produce el problema?
- ¿Qué secuencia de sucesos conduce hasta el momento en que se informó del problema?
- ¿El problema se produce tras un cambio del entorno, como una actualización o instalación de software o de hardware?

Responder a estos tipos de preguntas puede proporcionarle un marco de referencia en el cual investigar el problema.

¿En qué condiciones se produce el problema?

Es importante saber qué sistemas y aplicaciones están en ejecución cuando se produce el problema para resolverlo. Estas preguntas sobre el entorno pueden ayudarle a identificar la causa raíz del problema:

- ¿El problema se produce siempre cuando se realiza la misma tarea?
- ¿Tiene que producirse una secuencia de sucesos determinada para que aparezca el problema?
- ¿Hay alguna otra aplicación que falle al mismo tiempo?

Responder a este tipo de preguntas puede ayudarle a describir el entorno en el que se produce el problema y correlacionar dependencias. Recuerde que sólo porque varios problemas se hayan producido al mismo tiempo, no tienen por qué estar necesariamente relacionados.

¿Se puede reproducir el problema?

Desde el punto de vista de la resolución de problemas, un problema ideal es el que se puede reproducir. Por lo general, cuando se puede reproducir un problema se dispone de un conjunto más grande de herramientas o procedimientos que facilitan la investigación. Por consiguiente, los problemas que se pueden reproducir suelen se más fáciles de depurar y resolver.Sin embargo, los problemas que puede reproducir pueden tener una desventaja: si el problema tiene un impacto empresarial significativo, no querrá que se reproduzca. Si es posible, vuelva a producir el problema en un entorno de prueba o desarrollo, lo cual suele ofrecer más flexibilidad y control durante la investigación.

- ¿Se puede volver a crear el problema en un sistema de prueba?
- ¿Hay varios usuarios o aplicaciones que encuentren el mismo tipo de problema?
- ¿Se puede volver a crear el problema ejecutando un solo mandato, una serie de mandatos o bien una aplicación específica?

Información relacionada

"Búsqueda en bases de conocimiento" en la página 330
A menudo puede encontrar la solución al problema realizando búsquedas en las bases de conocimiento de IBM. Puede optimizar los resultados mediante los recursos, las herramientas de soporte y los métodos de búsqueda disponibles.

Habilitación de seguimientos y visualización de archivos de registros

Para solucionar un problema en IBM Intelligent Operations Center , es posible que tenga que analizar los archivos de registro en varios sistemas. Los siguientes temas le proporcionan orientación sobre cómo acceder a los archivos de registro.

Para iniciar el seguimiento y visualizar los registros, entre los mandatos en el tiempo de ejecución como usuario root.

Conceptos relacionados:

"Verificación de componentes" en la página 214
La herramienta Comprobación de verificación del sistema prueba componentes dentro de IBM Intelligent Operations Center para determinar si son accesibles y operativos.

"Instalación y utilización de IBM Support Assistant Lite" en la página 310
IBM Support Assistant Lite (ISA Lite) es una herramienta que recopila datos comunes de diagnóstico que son útiles para analizar problemas generales.

Tareas relacionadas:

"La ejecución de la instalación debe reunir la herramienta" en la página 305
Los archivos de registro se generan mientras se está instalando IBM Intelligent Operations Center . Hay una herramienta para recopilar estos archivos de registro para su análisis.

Archivos de registro de Servidor de aplicaciones

Utilice los procedimientos siguientes para habilitar rastreos y ver los registros para algunos de los sistemas de servidor de aplicaciones.

Los procedimientos siguientes describen cómo habilitar rastreos y ver registros para los siguientes sistemas:

- WebSphere Portal
- IBM WebSphere Business Monitor

Habilitación de rastreo y visualización de registros enWebSphere Portal

Acerca de esta tarea

Los registros de WebSphere Portal están en `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal`. Siga los pasos del procedimiento para iniciar un rastreo y ver un registro.

Procedimiento

1. Inicie sesión en la consola administrativa en http://**app-host**:9060/ibm/console, donde **app-host** es el nombre de host completo de servidor de aplicaciones.
2. Pulse **Resolución de problemas** > **Registros y rastreo**.
3. Pulse **WebSphere_Portal** > **Cambiar detalles de nivel de registro**.
4. Pulse la pestaña **Tiempo de ejecución** y pegue el siguiente mandato:
   ```
   *=warning: com.ibm.iss.*=all: com.ibm.ioc.*=all
   ```
5. Pulse **Aceptar**.
6. Para ver un registro, entre los siguientes mandatos:
   ```
   cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal
   tail –f trace.log
   ```

Habilitación de rastreo y visualización de registros para IBM WebSphere Business Monitor en servidor de aplicaciones

Acerca de esta tarea

Los registros para IBM WebSphere Business Monitor en servidor de aplicaciones están ubicados en`/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/`. Siga los pasos del procedimiento para iniciar un rastreo y ver un registro.

Procedimiento

1. Inicie sesión en la consola administrativa en http://**app-host**:9060/ibm/console, donde **app-host** es el nombre de host completo de servidor de aplicaciones.
2. Pulse **Resolución de problemas** > **Registros y rastreo**.
3. Pulse **WBM_DE.AppTarget.WBMNode1.0** > **Cambiar detalles de nivel de registro**.
4. Haga clic en la pestaña **Tiempo de ejecución** y copie el siguiente código de nivel de rastreo: `*=info: com.ibm.wbm.*=finest: com.ibm.events.*=all: com.ibm.wbimonitor.xsp.cei.*=all: com.ibm.wbimonitor.xsp.eventselector.*=all`
5. Haga clic en **Aceptar**.

Información relacionada:

Documentación del producto IBM WebSphere Portal 7

Archivos de registro de Servidor de sucesos

Utilice los procedimientos siguientes para habilitar rastreos y ver los registros para algunos de los sistemas de servidor de sucesos.

Los procedimientos siguientes describen cómo habilitar rastreos y ver registros para los siguientes sistemas:

- Tivoli Service Request Manager
- WebSphere MQ y WebSphere Message Broker
- Analizador XML de Tivoli Netcool/OMNIbus
- Base de datos de Tivoli Netcool/OMNIbus (servidor de objetos)
- Base de datos de Tivoli Netcool/OMNIbus (agente de proceso)
- Tivoli Netcool/Impact

Habilitación de rastreo y visualización de archivos de registro para Tivoli Service Request Manager

Acerca de esta tarea

Utilice el siguiente procedimiento para depurar el flujo de información de Tivoli Service Request Manager para IBM Intelligent Operations Center.

Procedimiento

1. En la interfaz de usuario de Tivoli Service Request Manager , pulse **Ir a** > **Configuración del sistema** > **Configuración de plataforma** > **Inicio de sesión**.
2. En Registradores de raíz, del campo de filtro, entre `integración`.
3. Expanda **integración** .
4. Configure el registrador de integración:
   a. En **Nivel de registro**, pulse el icono **Seleccionar valor** . En la ventana Seleccionar valor , pulse **DEBUG**.
   b. En **Agregadores**, pulse el icono **Gestionar agregadores** . En la ventana Gestionar agregadores , seleccione la casilla de verificación**Dailyrolling** y, después, pulse **Aceptar**.

c. Seleccione la casilla de verificación **¿Activo?** .
d. Pulse el icono **Guardar registrador** .

5. En la lista **Seleccionar acción** , seleccione **Establecer carpeta raíz de registro**.
6. En la ventana Establecer carpeta raíz de registro, en **Carpeta raíz de registro**, escriba `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/` y, a continuación, haga clic en**Aceptar**.
7. Pulse el icono **Guardar registrador** .
8. En la lista **Seleccionar acción** , seleccione **Aplicar configuración**.
9. Para ver el registro, en un terminal de servidor Tivoli Service Request Manager , escriba los siguientes mandatos:

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/maximo/logs
tail -f event-host_MXServer_maximo_scheduled.log
```

donde *event-host* es el nombre de host deservidor de sucesos.

Tareas relacionadas:

"Comprobación de los archivos de registro" en la página 347
Compruebe el archivo de registro de políticas de Tivoli Netcool/OMNIbus y el archivo de registro deTivoli Service Request Manager.

Habilitación de rastreo y visualización de archivos de registro para WebSphere MQ y WebSphere Message Broker

Acerca de esta tarea

Los registros para WebSphere MQ y WebSphere Message Broker se almacenan en las siguientes ubicaciones:

- `/var/mqm/errors`
- `/var/mqm/qmgrs/IOC!MB!QM/errors`

Los archivos de rastro se graban en el directorio `/var/mqm/trace` . Puede activar el rastreo de un solo gestor de colas o de todos los gestores de colas, como se muestra en el siguiente procedimiento.

Procedimiento

1. Para iniciar, terminar o dar formato a un rastreo, elija el mandato apropiado:
   - Para iniciar un rastreo de todos los procesos, entre el siguiente mandato: `strmqtrc-e`
   - Para iniciar un rastreo para el gestor de colas IBM Intelligent Operations Center , entre el siguiente mandato: `strmqtrc m IOC.MB.QM`
   - Para iniciar un rastreo de mucho detalle para el gestor de colas IBM Intelligent Operations Center , entre el siguiente mandato:`strmqtrc -t all -t detail -m IOC.MB.QM`
   - Para finalizar todos los rastreos, entre el siguiente mandato: `endmqtrc -a`
   - Para dar formato a archivos de rastreo binarios en formato ASCII, entre el siguiente mandato: `dspmqtrc *.TRC`
2. Para comprobar el estado de WebSphere Message Broker:
   a. Entre el siguiente mandato: `ps -ef | grep IOC_BROKER`
   b. Para comprobar el estado de los procesos siguientes:
      - `bipservice IOC_BROKER`
      - `bipbroker IOC_BROKER`
      - `biphttplistener IOC_BROKER`
      - `DataFlowEngine IOC_BROKER 5fe69373-2f01-0000-0080-9ab9c3579b15 default`

Habilitación de rastreo y visualización de archivos de registro para el analizador XML de Tivoli Netcool/OMNIbus

Acerca de esta tarea

Los registros de WebSphere Portal están ubicados en `/opt/IBM/netcool/omnibus/log/ioc_xml.log`. Siga los pasos del procedimiento para iniciar un rastreo y ver un registro.

Procedimiento

1. Abra un terminal en servidor de sucesos.
2. Entre el siguiente mandato: `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`
3. Si no se muestra el mensaje `Connection status OK` en la parte inferior del archivo, para cambiar el nombre del archivo de registros actual, entre el siguiente mandato: `mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log`
4. Si no se muestra el mensaje `Connection status OK` , es posible que también vea el mensaje `Probe shutting down`. Para reiniciar el analizador, entre el siguiente mandato:
   `/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &`
5. Después de aproximadamente un minuto, entre el siguiente mandato de nuevo: `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`
6. Si el mensaje `Connection status OK` sigue sin mostrarse, compruebe el archivo `/opt/IBM/netcool/omnibus/log/ioc_xml.log` en busca de errores. Un problema de conexión podría significar que el servidor de objetos está caído. Consulte la siguiente sección, *Habilitación de rastreo y visualización de registros para la base de datos de Tivoli Netcool/OMNIbus (servidor de objetos)* .

Habilitación de rastreo y visualización de archivos de registro para la base de datos de Tivoli Netcool/OMNIbus (servidor de objetos)

Acerca de esta tarea

Los archivos de registro se encuentran en las siguientes ubicaciones:

- `/opt/IBM/netcool/omnibus/log/ioc_xml.log`
- `/opt/IBM/netcool/omnibus/log/NCOMS*.*`, por ejemplo:
  - `/opt/IBM/netcool/omnibus/log/NCOMS.log`
  - `/opt/IBM/netcool/omnibus/log/NCOMS_trigger_stats.log1`
  - `/opt/IBM/netcool/omnibus/log/NCOMS_profiler_report.log1`

Siga los pasos del procedimiento para iniciar un rastreo y ver un registro.

Procedimiento

1. Inicie sesión en una terminal como usuario root.
2. Entre el siguiente mandato: `/opt/IBM/netcool/omnibus/bin/nco_config &`
3. Si se le pregunta si desea importar desde `omni.dat`, pulse **sí** y, a continuación, pulse **finalizar**.
4. Minimice la ventana del agente de procesos.
5. Pulse con el botón derecho del ratón sobre **NCOMs**.
6. Seleccione la opción adecuada:
   - Si no se muestra la opción **Conectar como...** , debe iniciar el servidor de objetos NCOMS:
     a. Para iniciar el servidor de objetos NCOMS, cierre nco_config y entre el siguiente mandato: `/opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &`
     b. Si el servidor de objetos NCOMS no se inicia, busque un archivo `NCOMS.pid` en el directorio `/opt/IBM/netcool/omnibus/var` y suprímalo, a continuación, intente iniciar el servidor de nuevo.
   - Si se muestra la opción **Conectar como...** , pulse **Conectar como...**, a continuación, para el nombre de usuario, entre `root` y la contraseña.

7. Una vez ha iniciado el servidor NCOMs, para reiniciar el analizador, entre el siguiente mandato:
   ```
   /opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
   ```
8. Para ver el archivo de registros, entre el siguiente mandato: `tail -f /opt/IBM/netcool/omnibus/log/NCOMS.log`

Archivo de registro de base de datos de Tivoli Netcool/OMNIbus (agente de proceso)

El archivo de registros de base de datos Tivoli Netcool/OMNIbus (agente de procesos) está ubicado en`/opt/IBM/netcool/omnibus/log/NCO_PA.log`.

Habilitación y visualización de archivos de registro de Tivoli Netcool/Impact

Acerca de esta tarea

El archivo de registros está ubicado en `opt/IBM/netcool/impact/log/`. Siga los pasos del procedimiento para iniciar un rastreo y ver un registro.

Procedimiento

1. Inicie sesión en la consola de administración de Tivoli Netcool/Impact en `http://`*`event-host`*`:9080/nci` con el nombre de usuario `admin`, donde *event-host* es el nombre completo de host deservidor de sucesos. Si no se muestra una solicitud de inicio de sesión, entre los siguientes mandatos en una ventana de terminal:
   ```
   su – netcool
   /opt/IBM/netcool/bin/ewas.sh start
   ```
2. En la ventana Estado de servicio, desplácese hacia abajo y asegúrese de que se están ejecutando los siguientes servicios, como indica el símbolo verde:
   - `IOC_CAP_Event_Reader`
   - `IOC_Notification_Reader`
3. También en la ventana Estado de servicio, pulse el icono **Ver registro** al lado de **PolicyLogger** para ver si hay errores mostrados en el registro.
4. Si hay uno o más errores en el registro, para obtener más detalles, consulte los archivos de registro en el siguiente directorio: `/opt/IBM/netcool/impact/log/`
5. Si necesita más detalles, consulte los niveles de registro más altos. Pulse **PolicyLogger** y, a continuación, establezca el valor de **Nivel de registro más alto** en 3 y seleccione las casillas de verificación adecuadas.

Qué hacer a continuación

Puede activar varios registros en tiempo de ejecución a través de la consola de administración de WebSphere Application Server . Para obtener más información acerca de la activación del rastreo del portal y otros rastreos disponibles en WebSphere Portal, consulte el enlace cerca del inicio del tema para la documentación del producto de WebSphere Portal y busque *Registro y rastreo*.

Tareas relacionadas:

"Comprobación de los archivos de registro" en la página 347
Compruebe el archivo de registro de políticas de Tivoli Netcool/OMNIbus y el archivo de registro deTivoli Service Request Manager.

La ejecución de la instalación debe reunir la herramienta

Los archivos de registro se generan mientras se está instalando IBM Intelligent Operations Center . Hay una herramienta para recopilar estos archivos de registro para su análisis.

Procedimiento

1. Inicie sesión servidor de instalación como `root` y abra una ventana de terminal.
2. Cambie al directorio *`install_home`*`/ioc/bin` .

3. Ejecute el mandato **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** para establecer la variable JAVA_HOME para utilizar el JER en tiempo de ejecución Java 6.
4. Ejecute el mandato **./mustgather.sh -p** *contraseña* donde *contraseña* es la contraseña de la topología. La herramienta explora el archivo de propiedades de topología la primera vez que se ejecuta. Si el archivo de propiedades de topología se cambia después de ejecutar la herramienta, añada **-n** al mandato para que la herramienta vuelva a explorar el archivo de propiedades de topología. Por ejemplo, **./mustgather.sh -n -p** *password*.

Resultados

Los archivos recopilados y demás información se graba en el directorio *install_media*/mustGather en servidor de instalación. Habrá un archivo con una extensión .tar para cada uno de los servidores.

La información recopilada incluye:

- Los registros de todas las fases, incluso los registros de los componentes instalados en los nodos.
- Registros de instalación de la herramienta Comprobación de verificación del sistema.
- Los archivos XML de topología.
- Todos los scripts utilizados durante el proceso de instalación.
- Todas las vulnerabilidades abordadas por Cyber Hygiene.
- Los scripts de Cyber Hygiene.

Conceptos relacionados:

"Habilitación de seguimientos y visualización de archivos de registros" en la página 301
Para solucionar un problema en IBM Intelligent Operations Center , es posible que tenga que analizar los archivos de registro en varios sistemas. Los siguientes temas le proporcionan orientación sobre cómo acceder a los archivos de registro.

"Resolución de problemas de los componentes"
Puede utilizar la herramienta Comprobación de verificación del sistema para resolver los problemas de los componentes en IBM Intelligent Operations Center.

Tareas relacionadas:

"Reinicio de la instalación de arquitectura IBM Intelligent Operations Center durante una instalación paso a paso" en la página 49
Si la instalación de arquitectura falla, se puede reiniciar la instalación.

"Intercambio de información con IBM" en la página 334
Para diagnosticar o identificar un problema, es posible que tenga que proporcionar al servicio de soporte de IBM datos e información sobre el sistema. En otros casos, el servicio de soporte de IBM le proporcionará herramientas o programas de utilidad que utilizar para la determinación de problemas.

Resolución de problemas de los componentes

Puede utilizar la herramienta Comprobación de verificación del sistema para resolver los problemas de los componentes en IBM Intelligent Operations Center.

Para obtener más información sobre la herramienta Comprobación de verificación del sistema , consulte el enlace al final del tema.

Las tablas de las siguientes secciones listan las ubicaciones del archivo de registro para cada servidor contenido en IBM Intelligent Operations Center. Todos los archivos de registro se crean automáticamente. Visualícelos utilizando los mandatos de cola adecuados.

Servidor de instalación

Para obtener información sobre la recopilación de los archivos de registro de instalación, consulte el tema acerca de la ejecución de información que debe recopilar la herramienta. Vaya al enlace al final del tema.

Servidor de aplicaciones

Tabla 96. Archivos de registro y componentes de Servidor de aplicaciones

Componente	Archivos de registro
IBM Cognos Administration	• /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Disp1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Disp1/SystemErr.log • /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemErr.log • Todos los registros del directorio /opt/IBM/cognos/c10_64/logs/
IBM HTTP Server	• /opt/IBM/HTTPServer/logs/error_log • /opt/IBM/HTTPServer/logs/access_log
IBM WebSphere Business Monitor	• /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log
IBM Lotus Sametime Proxy Server	• /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log
Tivoli Access Manager	• /var/pdweb/log/msg__*.log donde * es cualquier valor. • /var/pdweb/log/config_data__*.log donde * es cualquier valor
Tivoli Access Manager WebSEAL	• /var/pdweb/log/msg__webseald-default.log • Todos los registros del directorio /var/pdweb/www-default/log/
Registro de configuración del proxy Tivoli Directory Server	• /datahome/proxy/idsslapd-tdsproxy/logs/ibmslapd.log
WebSphere Operational Decision Management	• /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log
WebSphere Portal	• /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log • /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
WebSphere UDDI Registry	• /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log

Servidor de datos

Tabla 97. Archivos de registro y componentes de Servidor de datos

Componente	Archivos de registro
Tivoli Directory Server	• /datahome/dsrdbm01/idsslapd- dsrdbm01/logs/ibmslapd.log • Todos los registros del directorio /datahome/dsrdbm01 /idsslapd- dsrdbm01/logs/

Servidor de sucesos

Tabla 98. Archivos de registro y componentes de Servidor de sucesos

Componente	Archivos de registro
Lotus Domino	• /local/notesdata/console.out • /local/notesdata/log.nsf • Todos los registros en el directorio /local/notesdata/IBM_TECHNICAL_SUPPORT/.
Lotus Sametime Community Server	Para recopilar y escribir todos los archivos de registro pertinentes para el directorio /local/notesdata/ , entre el siguiente mandato: /local/notesdata/sh stdiagzip.sh
Tivoli Netcool/Impact	• /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemOut.log • /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemErr.log
Tivoli Netcool/OMNIbus	• /opt/IBM/netcool/log • /opt/IBM/netcool/omnibus/log
Tivoli Service Request Manager	• /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log • /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log

Servidor de gestión

Tabla 99. Archivos de registro y componentes de Servidor de gestión

Componente	Archivos de registro
Servidor de gestión	• Tivoli Event Monitoring Server: `/opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_ms_{nnnnnnn}.log` • Tivoli Event Portal Server: `/opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_cq_{nnnnnnn}.log` • Registros de WebSphere Application Server incorporado: – Registro de errores: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log` – Registro de salida: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log` – Registro de inicio: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/startServer.log`
Tivoli Access Manager y WebSphere Portal Manager	• `/var/PolicyDirector/log/msg__pdmgrd_utf8.log` • `/var/PolicyDirector/log/msg__pdacld_utf8.log`
Tivoli Access Manager	• `/opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log` • `/opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log`
Tivoli Enterprise Monitoring Agent	• `/opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnnn}.log`
Tivoli Enterprise Portal	• `/opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnnn}.log`
Tivoli Identity Manager	• `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log` • `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log` • Todos los registros del subdirectorio V6 del directorio `/var/idsldap/`

Conceptos relacionados:

"Gestión de archivos de registro" en la página 267
IBM Intelligent Operations Center almacena archivos de registro en varias ubicaciones diferentes. Para evitar problemas de rendimiento del sistema, archive periódicamente los archivos de registro y elimine los archivos de registro originales.

Tareas relacionadas:

"La ejecución de la instalación debe reunir la herramienta" en la página 305
Los archivos de registro se generan mientras se está instalando IBM Intelligent Operations Center . Hay una herramienta para recopilar estos archivos de registro para su análisis.

Información relacionada:

Cómo utilizar la herramienta de comprobación de verificación del sistema
La herramienta Comprobación de verificación del sistema se utiliza para determinar el estado operativo de los servicios que forman el sistemaIBM Intelligent Operations Center.

Instalación y utilización de IBM Support Assistant Lite

IBM Support Assistant Lite (ISA Lite) es una herramienta que recopila datos comunes de diagnóstico que son útiles para analizar problemas generales.

ISA Lite recopila los siguientes tipos de información:

- Archivos de determinación de problemas de plataforma
- Archivos de rastreo y de registro del sistema
- Archivos de suministro de plataformas
- Archivos de configuración del sistema
- Archivos de volcado de Java™
- Archivos de registro internos de infraestructura para determinación de problemas

Para descargar ISA Lite para IBM Intelligent Operations Center 1.5, consulte el enlace al final de este tema.

Para instalar y utilizar ISA Lite, siga las instrucciones de la guía de inicio rápido incluida en el paquete de descarga.

Información relacionada:

Descargando IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5

Mensajes de IBM Intelligent Operations Center

Cada uno de los temas de mensaje le ayuda a identificar la causas de una condición de error concreta en IBM Intelligent Operations Center y le recomienda acciones que debe tomar para resolver el error.

Para ayudarle a entender los errores que puede encontrarse al utilizar IBM Intelligent Operations Center, cada tema de mensaje se divide en tres secciones: el mensajes que se muestra en IBM Intelligent Operations Center o su registro, una explicación y una acción.

El mensaje
: Contiene dos identificadores, que son la identificación del error y el texto asociado. La identificación del error es el ID del mensaje. Es un número único que identifica un mensaje. El carácter final de E indica que el mensaje es resultado de un error, W indica un mensaje de advertencia y una I indica un mensaje informativo.

Descripción
: Contiene una explicación adicional del mensaje.

La respuesta del usuario
Sugiere la acción correctiva para resolver el error.

Para ayudarle a buscar información acerca de un mensaje de error, entre el número ID del mensaje de error en el campo de búsqueda del Information Center.

Nota: Los temas de esta sección contienen únicamente mensajes que son específicos para IBM Intelligent Operations Center. Para todos los demás mensajes, consulte la documentación del producto.

CIYBA0101E El archivo de topología {0} no es válido.

Explicación: El instalador ha intentado validar el archivo de topología {0} y ha encontrado errores en el mismo. Estos errores pueden incluir:

- No están todos los componentes necesarios en el archivo de topología.
- Componentes de requisito previo no listados antes de los componentes dependientes.
- Los componentes que deberían estar desplegados de forma secuencial están en la stanza de desarrollo paralelo.

Respuesta del Usuario: Corrija el archivo de topología y vuelva a ejecutar la instalación.

CIYBA0102E No se han encontrado los archivos de topología o de especificaciones de topología.

Explicación: Cada topología de instalación tiene un archivo .xml y una especificación asociados. No se ha encontrado uno o ninguno de estos archivos.

Respuesta del Usuario: Asegúrese de que todos los archivos de instalación se hayan extraído en servidor de instalación. Compruebe que la propiedad `image.basedir.local` del archivo `custom.properties` se haya establecido en la ubicación correcta. El archivo `custom.properties` está en el subdirectorio `/resource` de servidor de instalación donde se ha extraído el paquete de instalación.

CIYBA0103E No existe el script {0} para instalar un componente.

Explicación: El programa de instalación ha intentado ubicar un script para un componente, pero no se ha encontrado el script.

Respuesta del Usuario: Compruebe que el soporte de instalación se haya extraído en servidor de instalación. Compruebe que el directorio base de haya configurado en el archivo `custom.properties`. El directorio base se utiliza para derivar la ubicación del script de instalación.

CIYBA0104E El archivo de topología contiene entradas no válidas.

Explicación: El instalador ha encontrado un error al leer el archivo de topología y crear las unidades desplegables para cada componente. Suele tratarse de un error interno, a no ser que se esté instalando una topología personalizada.

Es posible que el archivo de topología esté dañado o no se haya especificado correctamente.

Respuesta del Usuario: Compruebe el archivo de topología para los siguientes problemas:

- ID de componente duplicados.
- Falta el ID de componente o los atributos de tipo.
- Especificación de un atributo de conexión donde no existe componente padre.
- No se puede validar el esquema XML de la topología.

CIYBA0105E El archivo {0} no se ha encontrado.

Explicación: El programa de instalación no ha podido encontrar el archivo {0}.

Respuesta del Usuario: Asegúrese de que todos los archivos de instalación se hayan extraído en servidor de instalación. Compruebe que la propiedad `image.basedir.local` del archivo `custom.properties` se haya establecido en la ubicación de la recopilación. El archivo `custom.properties` está en el subdirectorio `/resource` de servidor de instalación donde se ha extraído el paquete de instalación.

CIYBA0106E No se ha podido guardar el archivo {0}.

Explicación: El programa de instalación ha intentado escribir en el archivo llamado {0} y se ha devuelto un error E/S.

Respuesta del Usuario: Compruebe que la ubicación especificada es accesible mediante el ID de usuario del programa de instalación. Asegúrese de que haya suficiente espacio en el disco y de que la partición no esté dañado.

CIYBA0107E La referencia de la propiedad {0} no se ha encontrado en el archivo de topología {1}

Explicación: Durante la instalación algunos de los componentes necesitan valores de propiedad del software de requisitos previos. Estos componentes utilizan referencias de propiedades del archivo de topología para determinar los valores de la propiedad

necesaria. La referencia de propiedad no se ha encontrado en el archivo de topología.

Respuesta del Usuario: El archivo de topología está dañado. Es posible que ediciones manuales hayan introducido entradas no válidas o que la instalación haya escrito un archivo de topología con valores incorrectos. Determine qué componentes se han instalado de forma incorrecta. Elimine los componentes instalados de forma incorrecta, corrija el archivo de topología y vuelva a instalarlo.

CIYBA0108E El componente {0} no se ha encontrado en el archivo de topología {1}.

Explicación: El programa de instalación esperaba encontrar el ID de componente {0} en el archivo de topología {1}. El ID de componente no se ha encontrado. El problema puede deberse a una dependencia especificada de forma incorrecta en un elemento de conexión de otro componente.

Respuesta del Usuario: Revise el archivo de topología para obtener referencias a {0}. Corrija los elementos de conexión incorrectos del componente {0} y vuelva a instalarlo.

CIYBA0109E La propiedad {0}.{1} del archivo de topología {2} no es válida.

Explicación: La propiedad no se encuentra en el archivo de topología o en un archivo de propiedades de especificaciones.

Respuesta del Usuario: Si falta, añada la propiedad al archivo de propiedades de especificaciones o el archivo de topología. Este error puede deberse a un error de escritura de la propiedad. Corrija el archivo de topología o el archivo de propiedades de especificaciones y repita la instalación.

CIYBA0110E La propiedad {0}.{1} del archivo de topología {2} no se encuentra.

Explicación: Un unidad desplegable hace referencia a otra unidad desplegable indicada por el rol {1}. O bien no se encuentra la unidad de despliegue dependiente o los roles no coinciden.

Respuesta del Usuario: El archivo de topología ha indicado que contiene referencias a la propiedad mostrada; sin embargo, la definición de la propiedad no se encuentra en el archivo de topología. Esta situación puede ocurrir cuando el archivo de topología se ha editado de forma manual y se ha eliminado un componente, pero todavía existen referencias al mismo.

CIYBA0111E No se puede recuperar el host maestro del componente {0}.

Explicación: Se debe asociar un componente de topología con un host de destino. Se ha especificado un componente de topología huérfano.

Respuesta del Usuario: Compruebe el componente de topología {0} y asegúrese de que tenga una secuencia de atributos de conexión que, en última instancia, tenga un componente con un atributo de host.

CIYBA0112E No se ha podido leer el archivo de topología {0}

Explicación: El programa de instalación no ha podido leer el archivo de topología especificado.

Respuesta del Usuario: Compruebe que el archivo de topología indicado esté en el directorio de instalación y que el programa de instalación pueda acceder al directorio.

CIYBA0113E No se ha podido guardar el archivo {0}.

Explicación: El programa de instalación no ha podido guardar el archivo indicado.

Respuesta del Usuario: Compruebe que el programa de instalación tenga acceso al directorio de instalación.

CIYBA0114E La propiedad {0}.{1} no se puede establecer.

Explicación: El programa de instalación no ha podido actualizar la propiedad indicada.

Respuesta del Usuario: El archivo de topología está dañado o se ha editado de forma manual y se han introducido valores de propiedad no válidos. Corrija el archivo de topología y vuelva a ejecutar la instalación.

CIYBA0115E No se encuentra el archivo de topología {0}.

Explicación: El programa de instalación no ha podido acceder al archivo de topología indicado.

Respuesta del Usuario: Compruebe que el archivo de topología esté en el directorio especificado por el programa de instalación y asegúrese de que el programa de instalación pueda acceder al directorio.

CIYBA0116E No se puede escribir en el archivo de propiedades {0}.

Explicación: El programa de instalación no ha podido grabar el archivo de propiedades indicado.

Respuesta del Usuario: Compruebe que el ID de usuario utilizado por el programa de instalación tenga acceso a los directorios temporales de los servidores de destino. El directorio de los servidores de destino donde se escribirán los scripts de instalación temporal se especifica mediante la propiedad `Unix.script.basedir.remote` del archivo `custom.properties`. Corrija este valor de propiedad si se ha especificado de forma incorrecta.

CIYBA0117E El instalador no ha podido crear el almacén de claves.

Explicación: El programa de instalación no ha podido crear el almacén de claves.

Respuesta del Usuario: Compruebe que el ID de usuario que utiliza el programa de instalación tenga acceso a todos los subdirectorios donde se han extraído los soportes de instalación.

CIYBA0118E El programa de instalación no ha podido acceder al almacén de claves con la contraseña proporcionada. La contraseña es incorrecta o el almacén de claves está dañado.

Explicación: El programa de instalación no ha podido acceder al almacén de claves.

Respuesta del Usuario: Compruebe que la contraseña proporcionada sea correcta y que el almacén de claves no esté dañado. Vuelva a crear el almacén de claves con una contraseña nueva volviendo a instalar la solución.

CIYBA0119E No se puede cifrar la propiedad {0} del archivo de topología {1}.

Explicación: El programa de instalación ha intentado cifrar la propiedad indicada utilizando la contraseña proporcionada en el archivo de topología y no ha podido hacerlo.

Respuesta del Usuario: Compruebe que el almacén de claves no esté dañado y que la contraseña de la topología sea correcta. Si es necesario, vuelva a crear el almacén de claves con una contraseña nueva volviéndolo a instalar.

CIYBA0120E No se puede cifrar la propiedad {0} del archivo de topología {1}

Explicación: No se ha podido leer y descifrar la propiedad indicada.

Respuesta del Usuario: Compruebe que el ID de usuario utilizado por el programa de instalación pueda acceder al archivo de topología indicado y que el archivo de topología esté en la ubicación esperada. Compruebe que la contraseña y la clave secreta sean correctas. Vuelva a ejecutar la instalación.

CIYBA0121E El archivo del almacén de claves {0} ya existe.

Explicación: Este error no se producirá utilizando la instalación de IBM Installation Manager. IBM Installation Manager controla el flujo de instalación y garantiza que no se intenta volver a generar el almacén de claves.

Respuesta del Usuario: Compruebe que la instalación todavía no se haya ejecutado. Vuelva a ejecutar el instalador cuando se haya eliminado el almacén de claves existente de un intento de instalación anterior.

CIYBA0122E El almacén de claves de la topología no existe. Ejecute el mandato createSecretKey.

Explicación: Este error no se producirá utilizando la instalación de IBM Installation Manager. La instalación de IBM Installation Manager acepta de forma automática la clave secreta y genera el almacén de claves.

Respuesta del Usuario: Si ejecuta un a instalación paso a paso, siga los pasos para crear un almacén de claves.

CIYBA0123E La topología {0} no se ha instalado completamente.

Explicación: El programa de instalación ha determinado que no se han instalado todos los componentes de la topología.

Respuesta del Usuario: Compruebe el archivo de topología y determine qué componentes no se han instalado. Reinicie la instalación.

CIYBA0124E El archivo de propiedades de {0} no se encuentra.

Explicación: El programa de instalación ha intentado leer el archivo de propiedades indicado. Sin embargo, no se encuentra el archivo.

Respuesta del Usuario: Compruebe que el paquete de instalación se haya extraído correctamente. Compruebe que el ID de usuario utilizado por el programa de instalación tenga acceso a todos los directorios donde se ha extraído el paquete.

CIYBA0125E No se puede escribir en el archivo de propiedades {0}

Explicación: El programa de instalación ha intentado actualizar un archivo con los valores de la variable de tiempo de ejecución y se ha devuelto una excepción E/S.

Respuesta del Usuario: Compruebe que la ubicación especificada sea accesible utilizando el ID de usuario del programa de instalación. Compruebe que hay suficiente espacio en el sistema de archivos y que la partición del disco no esté dañada.

CIYBA0126E No se puede establecer el valor de la propiedad {0} del archivo de topología {1}

Explicación: El programa de instalación no ha podido establecer el valor de propiedad especificado.

Respuesta del Usuario: Compruebe que la propiedad

del archivo de topología indicado tenga la sintaxis XML correcta. Compruebe que el archivo de topología no esté dañado o formado incorrectamente. Elimine los caracteres especiales del archivo y reinicie la instalación.

CIYBA0127E No se puede leer el archivo de especificación de la solución {0}

Explicación: El programa de instalación ha intentado leer el archivo indicado y se ha devuelto un error de E/S.

Respuesta del Usuario: Compruebe que el archivo exista en la ubicación especificada. Compruebe que el ID de usuario utilizado por el programa de instalación tenga acceso a todos los directorios donde se ha extraído el paquete.

CIYBA0128E No se ha podido guardar el archivo {0}.

Explicación: El programa de instalación ha intentado escribir el archivo indicado y se ha devuelto un error de archivo de E/S.

Respuesta del Usuario: Compruebe que la ubicación especificada sea accesible por el ID de usuario utilizado por el programa de instalación. Compruebe que haya suficiente espacio en el sistema de archivos y que la partición de disco no esté dañada.

CIYBA0129E No se puede leer el archivo del paquete de la solución {0}.

Explicación: El programa de instalación ha intentado leer el archivo indicado y se ha devuelto un error de E/S.

Respuesta del Usuario: Compruebe que el archivo exista en la ubicación especificada. Compruebe que el ID de usuario utilizado por el programa de instalación tenga acceso a todos los directorios donde se ha extraído el paquete.

CIYBA0130E El archivo del paquete de la solución : {0} no existe.

Explicación: El programa de instalación ha intentado leer el archivo indicado y se ha devuelto un error de E/S.

Respuesta del Usuario: Compruebe los permisos del archivo indicado en el mensaje. Asegúrese de que el ID de usuario utilizado por el programa de instalación tenga permiso para leer el archivo. Modifique los permiso de archivo si es necesario.

CIYBA0131E El instalador no ha podido cargar el archivo de topología {0}. El mensaje de E/S del archivo era {1}.

Explicación: El error indicado se ha devuelto al intentar importar el archivo de topología especificado.

Respuesta del Usuario: Compruebe que el archivo de topología indicado esté en el directorio correcto. Compruebe que el archivo de topología no contenga ningún carácter no válido. Compruebe que el programa de instalación pueda acceder al directorio que contiene el archivo de topología.

CIYBA0140E NO se puede acceder a los archivos de instalación necesarios.

Explicación: El programa de instalación ha intentado leer un archivo necesario y no ha podido hacerlo.

Respuesta del Usuario: Compruebe que la ubicación donde se ha extraído el paquete de instalación sea accesible por el ID de usuario utilizado por el programa de instalación. Asegúrese de que la partición de disco no esté corrupta. Extraiga el paquete de instalación de nuevo y vuelva a ejecutar la instalación.

CIYBA0141E No se puede ubicar el archivo de instalación {0}.

Explicación: El programa de instalación ha intentado leer el archivo indicado y se ha devuelto un error de E/S.

Respuesta del Usuario: Compruebe que el archivo exista en la ubicación especificada. Compruebe que el ID de usuario utilizado por el programa de instalación pueda acceder a todos los directorios que contienen el paquete de instalación extraído.

CIYBA0142E No se puede escribir en el archivo de instalación {0}.

Explicación: El programa de instalación ha intentado escribir en el archivo indicado y se ha devuelto un error de E/S de archivo.

Respuesta del Usuario: Compruebe que el ID de usuario utilizado por el programa de instalación pueda acceder a todos los directorios que contienen el paquete de instalación extraído. Compruebe que la partición del disco no esté dañado y no se haya quedado sin espacio.

CIYBA0143E El programa de instalación no ha podido procesar el archivo de topología.

Explicación: El programa de instalación lee el archivo de topología y genera archivos intermedios con valores de tiempo de ejecución. El programa de instalación ha detectado un error al procesar el archivo de topología y escribir los archivos intermedios. Es probable que los errores de E/S de archivo sean la causa de este error.

Respuesta del Usuario: Compruebe que el ID de usuario utilizado por el programa de instalación tenga acceso a todos los directorios donde se ha extraído el paquete de instalación. Compruebe que la partición del disco no esté dañada y que tenga suficiente espacio.

CIYBA0150E No se puede leer el archivo de especificación de la topología {0}.

Explicación: El programa de instalación ha intentado leer el archivo indicado y se ha devuelto un E/S de archivo.

Respuesta del Usuario: Compruebe que el archivo exista en la ubicación especificada. Compruebe que el ID de usuario utilizado por el programa de instalación tenga acceso a todos los directorios donde se ha extraído el paquete de instalación.

CIYBA0160E El archivo de especificación de reglas no se ha encontrado en el directorio {0}.

Explicación: El programa de instalación ha intentado cargar el archivo `rule-spec.xml` que define las reglas de comprobación previa y no ha podido hacerlo.

Respuesta del Usuario: Compruebe que existe el directorio indicado. Asegúrese también de que el ID de usuario utilizado por el programa de instalación pueda acceder al directorio.

CIYBA0161E El nombre de regla {0} no es válido.

Explicación: El programa de instalación ha identificado un nombre de regla incorrecto en el archivo `rule-spec.xml`. Este archivo define las reglas utilizadas por el paso de comprobación previa.

Respuesta del Usuario: Compruebe que el nombre de la regla sea correcto en el archivo `rule-spec.xml`. Consulte una versión sin cambios del archivo `rule-spec.xml` para consultar el nombre de regla correcto.

CIYBA0162E La comprobación de requisitos previos de instalación ha fallado para la topología {0}.

Explicación: El paso de comprobación previa ha fallado porque uno o más destinos de configuración no cumplen los requisitos de sistema soportados.

Respuesta del Usuario: Compruebe que la topología planificada cumpla los requisitos soportados mínimos.

CIYBA0163W El tipo de SO del servidor de destino {0} no es {1}.

Explicación: El paso de comprobación previa ha detectado un sistema operativo no compatible en el servidor de destino indicado.

Respuesta del Usuario: Asegúrese de que el sistema operativo en el servidor de destino cumple los requisitos de sistema soportados.

CIYBA0164W Se espera que el servidor {0} tenga un SO bit {1}.

Explicación: El paso de comprobación previa ha detectado un sistema operativo incorrecto en el servidor de destino.

Respuesta del Usuario: Compruebe que el tipo de sistema operativo en el servidor de destino cumple los requisitos del sistema.

CIYBA0165W La CPU del servidor de destino {0} no es una CPU x86 o s390 64 bits.

Explicación: El paso de comprobación previa ha detectado un tipo de CPU no admitido para el servidor de destino indicado.

Respuesta del Usuario: Compruebe que el tipo de CPU para el servidor de destino cumple los requisitos del sistema.

CIYBA0166E No se puede conectar con el servidor de destino {0}.

Explicación: El programa de instalación no ha podido conectarse con el servidor remoto al ejecutar el paso de comprobación previa.

Respuesta del Usuario: Compruebe la conectividad entre servidor de instalación y los servidores de destino. Compruebe los registros de comprobación previa para buscar otros errores.

CIYBA0167E No se puede conectar con el servidor {0} porque el nombre de host, la cuenta o la contraseña especificados son erróneos.

Explicación: El programa de instalación ha fallado al ejecutar el paso de comprobación previa. El programa de instalación no ha podido conectarse con el servidor de destino.

Respuesta del Usuario: Compruebe que el nombre de host tenga el formato correcto y que los detalles de inicio de sesión sean correctos para el servidor remoto. Compruebe los registros de comprobación previa para obtener información adicional.

CIYBA0168E La hora o la zona horaria de los servidores {0} y {0} no están sincronizadas.

Explicación: Hay diferencias entre la hora o las zonas horarias establecidas para los servidores.

Respuesta del Usuario: Compruebe que la hora y la zona horaria sean iguales para todos los servidores.

CIYBA0169W Compruebe el tipo de SO y la arquitectura de CPU en el servidor {0}

Explicación: El paso de comprobación previa del programa de instalación ha encontrado un sistema operativo y una arquitectura de CPU no soportados para un servidor de destino.

Respuesta del Usuario: Asegúrese de que todos los servidores cumplan los requisitos de sistema de la solución.

CIYBA0170W Compruebe la zona horaria y la fecha y & hora en todos los servidores

Explicación: Este mensaje va seguido de la palabra "válido" o "no válido". Lo indicado determina la acción que se realizará.

Respuesta del Usuario: Si el mensaje va seguido de "válidos", no se necesita ninguna respuesta. Si el mensaje va seguido de "no válido", los servidores se deben sincronizar. Los parámetros de zona horaria, fecha y hora del sistema deben ser iguales para cada nodo de la topología.

CIYBA0171I Se está iniciando la comprobación de requisitos previos de instalación utilizando la instancia {0}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0172I La comprobación de requisitos previos de instalación ha finalizado correctamente.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0173I La comprobación de requisitos previos de instalación ha finalizado con {0} advertencias y {1} errores:

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0176E La información de inicio de sesión del servidor {0} es incorrecta. Compruebe el ID de usuario y la contraseña para el servidor.

Explicación: El paso de comprobación previa del programa de instalación ha encontrado información de inicio de sesión incorrecta para el servidor de destino.

Respuesta del Usuario: Compruebe que los datos de la cuenta para el servidor tengan el ID de usuario y la contraseña correctos.

CIYBA0177W No se puede conectar con el servidor remoto. Esperando para reintentar.

Explicación: El paso de comprobación previa del programa de instalación no ha podido conectarse con el servidor remoto. La conexión se volverá a intentar.

Respuesta del Usuario: No es necesaria ninguna acción.El programa de instalación esperará la cantidad de tiempo especificada en la propiedad `waiting.time` del archivo `custom.properties` y, a continuación, volverá a intentar la conexión.

CIYBA0178W No se puede establecer conexión con {0}, se esperarán {1} milisegundos antes del siguiente intento de conexión.

Explicación: Hay problemas de conectividad en el sistema.

Respuesta del Usuario: Si fallan varios intentos de conexión, póngase en contacto con el administrador de red para resolver los problemas de conectividad y vuelva a intentar la instalación.

CIYBA0179E No se ha proporcionado ningún valor para la clave {0} en el archivo de propiedades de topología.

Explicación: El paso de comprobación previa del programa de instalación no ha podido recuperar los valores del nombre de host, nombre de usuario o contraseña desde el archivo de propiedades.

Respuesta del Usuario: Compruebe que el nombre de host, el nombre de usuario y la contraseña se hayan especificado correctamente en el archivo de propiedades.

CIYBA0180E El ID de usuario introducido para el servidor {0} no tiene privilegios raíz.

Explicación: El paso de comprobación previa del programa de instalación ha detectado que la cuenta utilizada para el servidor indicado no tiene privilegios raíz.

Respuesta del Usuario: Cambie el ID de usuario utilizado para el servidor a uno que tenga privilegios raíz o añada privilegios raíz al usuario especificado para el servidor.

CIYBA0181E Verifique el ID de usuario raíz y la contraseña para el servidor {0}.

Explicación: El paso de comprobación previa del programa de instalación ha determinado que el ID de usuario utilizado para el servidor tiene unos derechos de acceso insuficientes.

Respuesta del Usuario: Compruebe que la cuenta tenga suficientes derechos de acceso.

CIYBA0182E Compruebe la conectividad del servidor de instalación con {0}

Explicación: El paso de comprobación previa del programa de instalación no ha podido establecer la conexión entre servidor de instalación y el servidor de destino.

Respuesta del Usuario: Compruebe la conectividad entre servidores. Revise los registros de comprobación previa para obtener información adicional.

CIYBA0183E El valor {0} de la clave {1} no es válido, debería ser "EM64T", "AMD64" o "S390".

Explicación: El valor de clave debe ser uno de los valores especificados.

Respuesta del Usuario: Corrija el valor y vuelva a ejecutar la instalación.

CIYBA0184E El valor {0} de la clave {1} no es un nombre de host válido.

Explicación: El paso de comprobación previa del programa de instalación ha determinado que el valor proporcionado no es un nombre de host válido.

Respuesta del Usuario: Compruebe que el formato y el valor del nombre de host sean correctos.

CIYBA0185E La comprobación de requisitos previos de instalación ha fallado en la regla {0}

Explicación: El paso de comprobación previa del programa de instalación ha fallado al comprobar la regla especificada.

Respuesta del Usuario: Compruebe los registros de comprobación previa de los mensajes de adición. Corrija el error y vuelva a intentar la instalación.

CIYBA0187E Se ha especificado el almacén de claves SSH "{0}", pero no se ha podido acceder. El protocolo SSH basado en certificado no estará disponible. Detalles: {1}.

Explicación: El paso de comprobación previa del programa de instalación ha detectado datos no válidos en el almacén de claves SSH al intentar conectarse al servidor de destino.

Respuesta del Usuario: Revise los detalles del mensaje y compruebe que el almacén de claves proporcionado tenga las entradas adecuadas.

CIYBA0190E El componente {0} debe aparecer antes del componente {1} en el archivo de topología.

Explicación: El archivo de topología se ha cambiado de forma incorrecta. Un componente de requisito previo aparece después de un componente que depende de él.

Respuesta del Usuario: Cambie el archivo de topología para que los componentes con dependencias estén después de los componentes de los que dependen.

CIYBA0191E Existe una dependencia ente el componente {0} y el componente {1} en el archivo de topología. Los componentes no se pueden desplegar en paralelo.

Explicación: Los componentes no se pueden desplegar en paralelo si existe una dependencia entre ellos. Por ejemplo, si el componente 2 es un requisito previo del componente 1.

Respuesta del Usuario: Elimine los componentes de la stanza paralela del archivo de topología.

CIYBA0192E La propiedad {1}.{2} tiene un valor de referencia no válido de {0} en el archivo de topología.

Explicación: El valor de referencia incluido en el mensaje no es válido para la propiedad indicada.

Respuesta del Usuario: Utilice el campo ID para buscar la definición de propiedad y asegúrese de que todas las referencias a la propiedad tengan el valor correcto.

CIYBA0193E El componente {0} tiene conexiones duplicadas {1} identificadas en el archivo de topología.

Explicación: Las conexiones duplicadas del componente están definidas en el archivo de topología.

Respuesta del Usuario: Elimine la información de conexión duplicada del archivo de topología y vuelva a ejecutar el programa de instalación.

CIYBA0194E La propiedad {0} está duplicada en el componente {0}

Explicación: Se ha definido una propiedad duplicada para el componente.

Respuesta del Usuario: Elimine la propiedad

duplicada del componente en el archivo de propiedades.

CIYBA0195E El componente {0} del archivo de topología tiene una propiedad no válida {0}.

Explicación: La propiedad especificada no se esperaba para el componente indicado. Esto podría deberse a una propiedad escrita incorrectamente o a una propiedad ausente de la especificación de propiedades.

Respuesta del Usuario: Añada la propiedad especificada al archivo de propiedades o de topología. Si la propiedad está mal escrita, corríjala. Corrija el archivo de topología o los archivos de propiedad de especificaciones y reinicie la instalación.

CIYBA0196E Al componente {1} le falta la propiedad {0}

Explicación: El componente debe tener la propiedad indicada. El error puede deberse a una propiedad escrita incorrectamente o a una propiedad ausente del archivo de especificaciones de propiedades.

Respuesta del Usuario: Añada la propiedad al archivo de propiedades de especificaciones o de topología. Si el error se debe a una falta de ortografía, corríjala. Reinicie la instalación.

CIYBA0197E El componente {1} tiene un tipo de componente no válido {1} especificado.

Explicación: Se ha especificado un tipo de componente no válido para el componente.

Respuesta del Usuario: Compruebe que el archivo de especificación del componente contenga el tipo de componente. Los archivos de especificación del componente se encuentran en el subdirectorio *inicio_instalación*/spec/*componente* de servidor de instalación.

CIYBA0198E La conexión {0} no es válida para el componente {1}

Explicación: La conexión definida no es válida para el componente.

Respuesta del Usuario: Compruebe la ortografía de la conexión en el archivo de topología del componente y asegúrese de que no esté mal escrito.

CIYBA0199E Faltaba la conexión {0} en el componente {1}.

Explicación: No se han definido ninguna conexión para el componente indicado.

Respuesta del Usuario: Compruebe el archivo de especificaciones del componente y asegúrese de que la información de conexión esté incluida.

CIYBA0200E La información de conexión de {0} no existe.

Explicación: Falta el ID de conexión para el componente indicado.

Respuesta del Usuario: Compruebe que el ID de conexión se haya especificado en el archivo de topología. Compruebe que el ID de conexión esté escrito correctamente y que haga referencia a una stanza del archivo de topología que defina el componente asociado para el ID de conexión.

CIYBA0201E No se puede conectar con el servidor remoto {0}.

Explicación: El programa de instalación ha encontrado un problema de conectividad con el servidor indicado.

Respuesta del Usuario: Compruebe que no haya problemas de conexión entre los servidores. Ejecute el paso de comprobación previa del programa de instalación y resuelva los problemas de conectividad.

CIYBA0202E El nombre de usuario o la contraseña no son válidos para el servidor {0}.

Explicación: El programa de instalación ha encontrado credenciales no válidas para el servidor indicado.

Respuesta del Usuario: Compruebe que las credenciales del servidor son correctas en el archivo de topología.

CIYBA0203E El archivo {0} no existe.

Explicación: Se ha intentado cargar el archivo de propiedades y se ha devuelto un error.

Respuesta del Usuario: Compruebe que la vía de acceso al archivo de propiedades sea correcta y que el archivo exista.

CIYBA0204E No se puede leer/escribir el archivo {0}.

Explicación: El programa de instalación ha intentado cargar el archivo de propiedades y se ha devuelto un error.

Respuesta del Usuario: Compruebe que la vía de acceso del archivo de propiedades sea correcta y que el archivo indicado exista.

CIYBA0205E No se puede crear el directorio {0} en {1}.

Explicación: El programa de instalación no ha podido crear un directorio en el servidor remoto.

Respuesta del Usuario: Compruebe que haya suficiente espacio en el servidor remoto y que el ID de usuario utilizado por el programa de instalación tenga suficientes derechos y los permisos adecuados para crear un directorio.

CIYBA0206E No se ha podido cargar el archivo {0} al directorio remoto {1} del servidor {2}.

Explicación: El programa de instalación no ha podido copiar archivos en el directorio indicado del servidor remoto.

Respuesta del Usuario: Compruebe que haya suficiente espacio en el servidor remoto y que el ID de usuario utilizado por el programa de instalación tenga suficientes derechos de acceso y los permisos adecuados para escribir archivos en el servidor remoto.

CIYBA0207E No se ha definido ninguna imagen para {0}.

Explicación: El programa de instalación no ha podido recuperar los datos de imagen del archivo de propiedades.

Respuesta del Usuario: Compruebe que el archivo de propiedades contenga un campo de imagen con el componente de datos.

CIYBA0208E No se puede cargar la imagen del componente {0} en el servidor remoto {1}.

Explicación: El programa de instalación no ha podido copiar los archivos de imagen en un directorio del servidor remoto.

Respuesta del Usuario: Compruebe que haya suficiente espacio en el servidor remoto y que el ID de usuario utilizado por el programa de instalación tenga suficientes derechos de acceso y los permisos adecuados para escribir en el directorio del servidor remoto. Compruebe también que el nombre del directorio remoto sea correcto.

CIYBA0209I Nombre de host : {0}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0210I OSType={0},OSBit={1},CPUArch={2}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0211I Vía de acceso remota : {0}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0212I Vía de acceso local : {0}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0213E No se puede descargar el archivo {0} del servidor remoto {1}.

Explicación: El programa de instalación no ha podido copiar los archivos de imagen desde un servidor de directorio remoto al servidor local.

Respuesta del Usuario: Compruebe que haya suficiente espacio en el servidor local y que el ID de usuario utilizado por el programa de instalación tenga suficientes derechos y los permisos adecuados para escribir en el directorio. Compruebe también que los nombres de los directorios locales y remotos sean correctos.

CIYBA0214E Descargue el archivo {0}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0215I Mandato : {0}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0216I Código de salida de mandato : {0}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0217I Salida del mandato : {0}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0218E El mandato ha fallado con el código de retorno {0}.

Explicación: El mandato no se ha completado correctamente.

Respuesta del Usuario: Compruebe los archivos de registro para obtener más detalles.

CIYBA0219I Cargue el archivo {0}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0220I Directorio de imagen local : {0}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0221I Directorio de imagen remota : {0}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0222E La imagen remota {0} ya existe.

Explicación: El archivo ya existe en el servidor de destino. El proceso de instalación incluye la transferencia de soportes a los servidores de destino. Este imagen indica que la imagen necesaria ya se ha transferido.

Respuesta del Usuario: Este mensaje indica que los soportes de un intento de instalación anterior todavía están en los servidores de destino. Si el usuario pretende iniciar una nueva instalación, los soportes se deben suprimir para poder cargarlos de nuevo.

CIYBA0223E No se puede iniciar el mandato en el servidor {0}.

Explicación: El programa de instalación no ha podido ejecutar el mandato **IOC** desde el servidor remoto en el servidor local.

Respuesta del Usuario: Compruebe la conexión entre el servidor local y el servidor remoto. Compruebe que el ID de usuario utilizado por el programa de instalación tenga suficientes derechos de acceso y los permisos adecuados para ejecutar un mandato.

CIYBA0224E Obtenga los archivos de copia de seguridad de la carpeta {0} en el servidor {1}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0225E No se pueden obtener los archivos de copia de seguridad desde la carpeta {0} en el servidor {1}.

Explicación: El programa de instalación no ha podido recuperar los archivos desde una carpeta de copia de seguridad remota a una carpeta local.

Respuesta del Usuario: Compruebe la conexión entre el servidor local y el servidor remoto. Compruebe que el ID de usuario utilizado por el programa de instalación tenga suficientes derechos de acceso y los permisos adecuados para acceder a las carpetas.

CIYBA0226E No hay ninguna carpeta de copia de seguridad {0} en el servidor {1}.

Explicación: El programa de instalación no ha podido recuperar los archivos desde una carpeta de copia de seguridad remota a una carpeta local.

Respuesta del Usuario: Compruebe que el directorio y la carpeta remotos existan.

CIYBA0227E Se debe proporcionar un valor para el ID y el atributo de vía de acceso.

Explicación: La instalación no ha podido identificar el ID de componente ni el atributo de vía de acceso.

Respuesta del Usuario: Compruebe que el ID de componente y los argumentos de vía de acceso se hayan proporcionado en los argumentos de tarea.

CIYBA0228I Ejecutar mandato: {0}.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0229E Espacio de disco insuficiente en el directorio de destino {0}.

Explicación: El programa de instalación no ha encontrado suficiente espacio de disco en el directorio de destino.

Respuesta del Usuario: Compruebe que el directorio indicado tenga suficiente espacio asignado y que sea accesible por el ID de usuario utilizado por el programa de instalación.

CIYBA0230I Versión de línea de mandatos IOC: {0}

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0231I Se ha importado correctamente la topología "{0}"

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0232E El nombre de topología "{0}" no se encuentra en la carpeta ../topology

Explicación: El programa de instalación no ha podido encontrar la topología indicada en la carpeta `../topology`.

Respuesta del Usuario: Compruebe que el archivo de topología exista en la carpeta `../topology` y que tenga un formato XML válido.

CIYBA0233I La topología actual es "{0}".

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0234E ANT_HOME no está establecido o se ha establecido de forma incorrecta. Establezca ANT_HOME.

Explicación: El programa de instalación ha encontrado un problema en la variable de entorno `ANT_HOME`.

Respuesta del Usuario: Compruebe que la variable de entorno `ANT_HOME` se haya establecido en una versión ANT válida.

CIYBA0237E El ID de componente "{0}" no es válido.

Explicación: El programa de instalación ha encontrado un ID de componente incorrecto en el archivo de topología.

Respuesta del Usuario: Compruebe que el ID de componente exista y que su nombre sea correcto en el archivo de topología.

CIYBA0238E La acción "{0}" del ID de componente "{1}" no es válida.

Explicación: La acción indicada es incorrecta para el componente actual del archivo de topología.

Respuesta del Usuario: Compruebe el archivo de topología y asegúrese de que la acción definida sea adecuada para el componente.

CIYBA0239E Si desea mensajes de operación más detallados, compruebe {0}.

Explicación: El mandato no se ha completado correctamente.

Respuesta del Usuario: Compruebe el archivo de registro indicado por {0} para consultar las acciones que se deben realizar.

CIYBA0240I El mandato ha finalizado correctamente.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0241E El mandato ha fallado :

Explicación: El mandato mostrado ha fallado.

Respuesta del Usuario: La acción que se realizará depende del mandato que ha fallado. Revise el mando y los registros para determinar la causa del error.

CIYBA0242E Elimine ".xml" del parámetro "{0}".

Explicación: El parámetro mostrado incluye la extensión del archivo `.xml`.

Respuesta del Usuario: Los parámetros de nombre de archivo XML no deben incluir la extensión `.xml`. Elimine `.xml` del parámetro y vuelva a intentar el mandato.

CIYBA0243E Las variables de entorno IOP_CIPHER_ALG o IOP_CIPHER_KEYSIZE se han establecido incorrectamente. Establezca los valores compatibles con JCE apropiados..

Explicación: El programa de instalación no ha podido identificar el valor correcto para el cifrado utilizado.

Respuesta del Usuario: Compruebe que los valores de entorno `CIPHER_ALG` y `IOP_CIPHER_KEYSIZE` se hayan establecido correctamente.

CIYBA0244E "{0}" no es un parámetro válido.

Explicación: El parámetro indicado no es un parámetro válido.

Respuesta del Usuario: Elimine o corrija el parámetro y vuelva a intentar el mandato.

CIYBA0245E "-{0}" falta el parámetro.

Explicación: El parámetro indicado es necesario, pero no está en el mandato.

Respuesta del Usuario: Vuelva a ejecutar el mandato incluyendo el parámetro que falta.

CIYBA0249I Preparar scripts de operación.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0250I Operación completada.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0251I Se ha iniciado la secuencia de operaciones.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0252I Se ha completado la secuencia de operaciones.

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0253I Cargue las imágenes [{0}] de componente al host [{1}]

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0254I Instale el componente [{0}] en el host [{1}]

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0255I Desinstale el componente [{0}] del host [{1}]

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0256I Inicie el componente [{0}] en el host [{1}]

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0257I Detenga el componente [{0}] en el host [{1}]

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0258I Propague el componente [{0}] en el host [{1}]

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0259I Aceptar

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0261I {0} tareas en ejecución

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0262I Se realizarán un total de {0} tareas

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0263I Realice una copia de seguridad del componente [{0}] en el host [{1}]

Explicación: Este mensaje solo tiene fines informativos.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0264E No se puede cargar el archivo de configuración de registro {0}.

Explicación: La función de registro no encuentra el archivo de propiedades que contiene los parámetros de configuración de registro.

Respuesta del Usuario: Compruebe que el paquete de instalación se haya extraído correctamente y que esté en un sistema de archivos al que pueda acceder el ID de usuario que ejecuta el programa de instalación.

CIYBA0265E No se puede crear el controlador de archivo para el registro.

Explicación: La función de registro ha intentado abrir un archivo utilizando un manejador de archivos de sistema y no ha podido hacerlo.

Respuesta del Usuario: Solicite al administrador del sistema que compruebe el número de manejadores de archivos disponibles para el sistema. Asegúrese de que el sistema de archivos donde se ha extraído el paquete de instalación no esté dañado.

CIYBA0266E El paquete RPM necesario {0} no está instalado en el servidor {1}.

Explicación: El paquete RPM indicado no se ha instalado en el servidor.

Respuesta del Usuario: Instale el paquete RPM en el servidor.

CIYBA0267E El servidor {1} no tiene suficiente espacio de disco. Se necesita {0} espacio de disco.

Explicación: El servidor no tiene suficiente espacio de disco o el servidor no cumple los requisitos del sistema para el espacio de disco.

Respuesta del Usuario: Suprima los archivos para liberar espacio en el servidor y cumplir los requisitos de espacio mínimo.

CIYBA0268E El servidor {1} no tiene suficiente memoria. Se necesitan {0} GB de memoria.

Explicación: No hay suficiente RAM en el servidor indicado. El servidor no cumple los requisitos de sistema sobre RAM mínima.

Respuesta del Usuario: Añada RAM al servidor.

CIYBA0269E No se puede crear el directorio {0} en el servidor {1}. El directorio ya existe.

Explicación: El directorio especificado ya existe en el servidor.

Respuesta del Usuario: Elimine el directorio del servidor.

CIYBA0270E El puerto TCP/IP {0} ya se está utilizando en el servidor {1}. Este puerto es necesario y debe estar disponible antes de la instalación.

Explicación: El programa o el proceso ya está configurado para utilizar un puerto TCP/IP necesario en el servidor.

Respuesta del Usuario: Vuelva a configurar el servidor para que el puerto necesario esté disponible. Vuelva a ejecutar la instalación.

CIYBA0271E El servidor {1} no tiene el nombre de host completo esperado. El nombre de host completo esperado es {0}.

Explicación: El servidor no tiene el nombre de host completo esperado.

Respuesta del Usuario: Si está utilizando la instalación de IBM Installation Manager, introduzca el nombre de host completo para el servidor. Si está utilizando la instalación paso a paso, introduzca el nombre de host completo en la sección `SERVERS` del archivo de propiedades de topología. Corrija el servidor listado en el mensaje de error.

CIYBA0272E La conexión de red del servidor {1} al servidor {0} se ha interrumpido.

Explicación: No hay conectividad de red entre los dos servidores indicados.

Respuesta del Usuario: Compruebe la conectividad entre los servidores. Si el problema continúa, póngase en contacto con el administrador de red del sistema.

CIYBA0273E El servidor {0} está ejecutando SELinux y no se soporta.

Explicación: SELinux no se soporta en IBM Intelligent Operations Center.

Respuesta del Usuario: Instale una versión compatible de Linux.

CIYBA0274E Se ha detectado un firewall activo en el servidor {0}. Se deben inhabilitar todos los firewalls antes de la instalación.

Explicación: El servidor tiene un firewall activo.

Respuesta del Usuario: Inhabilite el firewall del servidor durante la instalación.

CIYBA0275E No se puede encontrar una entrada DNS para el servidor {0}. La búsqueda DNS por IP o nombre de host ha fallado.

Explicación: El servidor no se ha configurado correctamente en el DNS o el DNS no funciona correctamente. El mandato de búsqueda DNS ha fallado para el servidor por dirección IP y nombre de host.

Respuesta del Usuario: Póngase en contacto con el administrador de red del sistema para el servidor y corrija la entrada DNS de DNS

CIYBA0276E El servidor {1} tiene una configuración de sistema que no cumple los requisitos de instalación. El número máximo de archivos abiertos [unlimit] es menos de {0}.

Explicación: La configuración del sistema para el número máximo de archivos abiertos no cumple los requisitos del sistema.

Respuesta del Usuario: La configuración **ulimit** debe modificarse al valor indicado.

CIYBA0277E La solicitud Linux encontrada no cumple los requisitos de instalación. El release esperado es {0}.

Explicación: El sistema operativo Linux instalado en el servidor indicado no se soporta.

Respuesta del Usuario: Instale una versión compatible de Linux.

CIYBA0278E La distribución de Linux encontrada no cumple los requisitos. La distribución esperada es {0}

Explicación: El sistema operativo Linux instalado no se soporta.

Respuesta del Usuario: Instale una distribución de Linux soportada.

CIYBA0279E El perfil de WebSphere Application Server {0} no se ha iniciado o la cuenta o contraseña no es válida en el servidor {4}.

Explicación: El perfil de WebSphere Application Server no se ha iniciado o se ha intentado iniciar con credenciales no válidas.

Respuesta del Usuario: Inicie el perfil deWebSphere Application Server utilizando un ID de usuario y contraseña correctos.

CIYBA0281E El servidor {0} no tiene habilitado IPv6. Habilite IPv6 en el servidor antes de la instalación.

Explicación: El servidor indicado no tiene configurado IPv6.

Respuesta del Usuario: Habilite IPv6 en el servidor indicado.

CIYBA0282E Algunos de los archivos ubicados en el directorio {0} del servidor de soportes están dañados.

Explicación: Todos los archivos de instalación tienen sumas de comprobación MD5 que se deben verificar antes de la instalación. La suma de comprobación MD5 en algunos archivos ubicados en el directorio indicado no tienen sumas de comprobación MD5 válidas.

Respuesta del Usuario: Extraiga el paquete de instalación de nuevo o vuelva a copiar los archivos en el directorio.

CIYBA0283E SSH en el servidor {0} no se ha configurado correctamente. La autenticación de contraseña mediante SSH es necesaria pero no se ha configurado en el servidor.

Explicación: La configuración SSH del servidor indicado es incorrecta.

Respuesta del Usuario: Vuelva a configurar el archivo `/etc/ssh/sshd_config` del siguiente modo:

- Elimine todas las sentencias `AllowUsers`.
- Especifique `YES` para `PermitRootLogin`.
- Especifique `YES` para `Password Authentication`.

Estos cambios sólo permiten a los usuarios `root` acceder al servidor utilizando SSH con la autenticación de contraseña.

CIYBA0284E {0} ha resultado ser un enlace [dinámico] simbólico. Los enlaces simbólicos no están permitidos.

Explicación: Los enlaces simbólicos o dinámicos a archivos o directorios no se soportan.

Respuesta del Usuario: Elimine los enlaces simbólicos y proporcione la vía de acceso directa o el nombre de archivo.

CIYBA0285E No se ha iniciado la instancia de Tivoli Directory Server {0} en el servidor {1}.

Explicación: La instancia de Tivoli Directory Server indicada se debe iniciar.

Respuesta del Usuario: Inicie Tivoli Directory Server.

CIYBA0286E La instancia de IBM DB2 {0} no se ha iniciado en el servidor {1}.

Explicación: La instancia de DB2 indicada no se ha iniciado.

Respuesta del Usuario: Inicie la instancia de DB2.

CIYBA0287E No se ha iniciado WebSphere Application Server {1} del perfil {0} en el servidor {2}.

Explicación: El perfil de WebSphere Application Server indicado no se ha iniciado en el servidor indicado.

Respuesta del Usuario: Inicie el perfil de WebSphere Application Server.

CIYBA0288E El servidor {0} no tiene "localhost" correlacionado con 127.0.0.1.

Explicación: En el archivo host de cada servidor, la entrada `localhost` se debe correlacionar con `127.0.0.1`.

Respuesta del Usuario: Actualice el archivo de host en el servidor para correlacionar el valor `localhost` con `127.0.0.1`.

CIYBA0289E El servidor {0} no tiene suficientes recursos de CPU. El recuento de recursos de CPU en el servidor es de {1}

Explicación: El servidor no tiene suficientes recursos de CPU para cumplir los requisitos.

Respuesta del Usuario: Añada recursos de CPU al servidor indicado.

CIYBA0301E Se ha pulsado un botón para ejecutar una prueba, pero no se han encontrado propiedades coincidentes en el archivo de propiedades.

Explicación: No se han encontrado las propiedades de la prueba en el archivo de propiedades.

Respuesta del Usuario: Pulse **Restablecer**. Esto hará que el programa lea el archivo de propiedades actual si se realizan cambios. Vuelva a intentar la prueba.

CIYBA0302E Cada prueba debe tener un número determinado de propiedades, la clase es una de ellas. Parámetros: {0}: nombre de clase {1}: nombre de método {2}: número de secuencia

Explicación: Falta la propiedad clase en la definición de la prueba.

Respuesta del Usuario: Busque el número de secuencia en el archivo de propiedades. Añada una propiedad de clase a la prueba. Este es el nombre de clase de la prueba. Este suele ser el nombre de clase del agente de ejecución remota (el código que reenvía la solicitud de prueba a `IopCatRemoteResponder` para la ejecución.

Por ejemplo:

```
0070.classname=com.ibm.iop.cat.fw.remote.IopCatRemoter
```

CIYBA0303E Cada prueba debe tener un número determinado de propiedades, la etiqueta de visualización es una de ellas. Parámetros: {0}: nombre de clase {1}: nombre de método {2}: número de secuencia

Explicación: Falta la definición de la prueba en la etiqueta de visualización.

Respuesta del Usuario: Busque el número de secuencia en el archivo de propiedades. Añada una propiedad `displaylabel` a la prueba. Este es el texto que se mostrará en el botón.

CIYBA0304E Se ha pulsado un botón para ejecutar una prueba, pero no se ha encontrado ninguna prueba coincidente en el archivo de propiedades.

Explicación: El archivo de propiedades cargado actualmente no define la prueba solicitada.

Respuesta del Usuario: Pulse **Restablecer**. Se volverá a cargar el archivo de propiedades actual.

CIYBA0305E Se ha pulsado un botón para ejecutar una prueba, pero no se encuentra la información de configuración de la prueba.

Explicación: La información de configuración no está disponible para la prueba.

Respuesta del Usuario: Pulse **Restablecer**. Se volverá a cargar el archivo de propiedades actual.

CIYBA0306E El código especificado por la clase no se ha encontrado. Parámetro:{0}: nombre de clase (no encontrado)

Explicación: No se ha especificado `classname` o no se ha encontrado el código.

Respuesta del Usuario: Compruebe las bibliotecas compartidas de la aplicación `IopCatRemoteResponder` para ver si falta una o más bibliotecas o si no se han especificado.

CIYBA0307E Las variables comunes se aplican a todas las pruebas.No se permite establecer el nombre, la clase o depuración utilizando común. Parámetros: {0}: nombre de clase {1}: nombre de método {2}: cadena de clave de propiedad

Explicación: `Common` se ha utilizado para establecer `name`, `class`, or `debug`.

Respuesta del Usuario: Busque la clave y elimine la línea conflictiva. Por ejemplo, `common.name` utilizado para denominar todas las pruebas con el mismo nombre.

CIYBA0308E Se ha producido una excepción en clase {0}, método {1}. Detalles {2}

Explicación: Se ha producido una excepción.

Respuesta del Usuario: Examine la cadena de excepción para determinar la causa del error de la prueba. Es posible que se trate de un error de prueba normal. Por ejemplo, "Conexión rechazada" suele significar que no había ningún programa escuchando en un puerto determinado y que, por tanto, el servicio no está en ejecución.

CIYBA0309E {0}.{1}() - Prueba[{2}] - Excepción: {3}

Explicación: Se ha producido una excepción de tiempo de ejecución en la prueba indicada.

Respuesta del Usuario: Revise el mensaje de error para obtener más información.

CIYBA0310E Se ha producido una excepción inesperada mientras se ejecutaba la prueba.

Explicación: Se ha producido una excepción inesperada.

Respuesta del Usuario: Revise otras excepciones para obtener detalles adicionales.

CIYBA0311I La cadena devuelta desde la prueba Echo de diagnóstico interno. Parámetro {0}: propiedades de entrada para la prueba.

Explicación: Muestra las propiedades de entrada de la prueba.

Respuesta del Usuario: Este es un mensaje normal y no una indicación de error.

CIYBA0312E La prueba web ha recibido el código de respuesta HTTP esperado (en 200"s o especificado por la propiedad expectedRcode). Parámetros: {0}: nombre de clase

Explicación: Indica que la prueba ha sido satisfactoria.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0313E La prueba web no ha recibido el código de respuesta HTTP esperado (en 200"s o especificado por la propiedad expectedRcode). Parámetros: {0}: nombre de clase {1}: código de respuesta HTTP

Explicación: Se ha recibido un código de respuesta HTTP inesperado.

Respuesta del Usuario: Compruebe la dirección URL especificada por la propiedad `hosturl` con un navegador o con el mandato **`wget`**.

CIYBA0314E La representación de la cadena de la respuesta de prueba. Parámetros: {0}: código de respuesta {1}: texto de respuesta {2}: texto específico de la prueba adicional

Explicación: Este mensaje devuelve la respuesta de prueba como una cadena.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYBA0315E Todas las pruebas deben tener propiedades. No se han pasado propiedades a esta prueba.

Explicación: Faltan propiedades de la invocación de la prueba.

Respuesta del Usuario: Este mensaje no debería recibirse porque la infraestructura ha pasado las propiedades. Póngase en contacto con IBM Software Support.

CIYBA0320E No se ha encontrado una cadena esperada en las propiedades del texto. Nombre de clase {0}, texto de salida {1}

Explicación: Las pruebas SSH inician sesión en el servidor, ejecutan los mandatos y buscan una cadena esperada en la salida de los mandatos. No se ha especificado ninguna cadena esperada en las propiedades de esta prueba.

Respuesta del Usuario: Busque la clave `expected` de la prueba. Añada o modifique la propiedad para especificar una cadena que se espera en la salida de los mandatos especificados en la propiedad `commmands`.

CIYBA0322E No se ha encontrado la cadena esperada en la salida.Nombre de clase {0}, texto de salida {1}

Explicación: Las pruebas SSH inician sesión en el servidor, ejecutan los mandatos y buscan una cadena esperada en la salida de los mandatos. La cadena esperada no se ha encontrado en la salida.

Respuesta del Usuario: Busque la clave `expected` de la prueba y del texto de salida. Esto podría indicar que la prueba ha fallado. Si el texto de salida contiene "teclado interactivo no permitido" podría significar que el ID de usuario o la contraseña utilizados para iniciar sesión en el servidor remoto son incorrectos. Compruebe las propiedades `user`, `password` y `hostname` de la prueba. La contraseña es un alias de una contraseña del almacén de claves.

CIYBA0323E Excepción inesperada en el nombre de clase {0}. Excepción: {1}

Explicación: Se ha producido una excepción inesperada.

Respuesta del Usuario: Si el texto de salida contiene "teclado interactivo no permitido" podría significar que el ID de usuario o la contraseña utilizados para iniciar sesión en el servidor remoto son incorrectos. Compruebe las propiedades `user`, `password` y `hostname` de la prueba. La contraseña es un alias de una contraseña del almacén de claves.

CIYBA0340E El agente de ejecución de pruebas (IopCatRemoteResponder) no ha podido analizar los datos JSON de entrada. Parámetros: {0}: nombre de clase {1}: nombre de método {2}: datos de envío

Explicación: La interfaz de usuario y el agente de ejecución de pruebas se comunican utilizando JSON. Este error significa que el agente de ejecución de pruebas (`IopCatRemoteResponder`) no ha podido analizar los datos JSON de entrada.

Respuesta del Usuario: Examine los datos de envío para comprobar si están en el formato JSON correcto.

CIYBA0341E Se ha encontrado una excepción mientras se ejecutaba la prueba.Parámetros: {0}: nombre de clase {1}: nombre de método {2}: cadena de excepción

Explicación: Se ha encontrado una excepción mientras se ejecutaba la prueba.

Respuesta del Usuario: Compruebe la cadena de excepción para determinar la causa del fallo de la prueba. Es posible que sea un error de prueba normal. Por ejemplo, "Conexión rechazada" suele significar que ningún programa escuchaba en el puerto y que el servicio no se está ejecutando.

CIYBA0342E El agente de ejecución de prueba (IopCatRemoteResponder) no ha podido enviar una respuesta a la interfaz de usuario. Parámetros: {0}: nombre de clase {1}: nombre de método {2}: cadena de excepción

Explicación: La interfaz de usuario y el agente de ejecución de pruebas se comunican utilizando JSON. Este error significa que el agente de ejecución de pruebas (`IopCatRemoteResponder`) no ha podido enviar una respuesta a la interfaz de usuario.

Respuesta del Usuario: Compruebe la cadena de excepción para determinar por qué no se puedo enviar la respuesta. Es posible que la prueba tardara demasiado y que la interfaz de usuario hubiera dejado de esperar.

CIYBA0343E Falta un prefijo clave esperado.Parámetros: {0}: nombre de clase {1}: nombre de método {2}: cadena de clave de propiedad

Explicación: Todas las propiedades de una prueba determinada tienen el mismo número como prefijo. Esto proporciona la agrupación porque los archivos de propiedades no son posicionales.

Respuesta del Usuario: Busque la clave en el archivo de propiedades y añada el prefijo apropiado. Por ejemplo, lo siguiente es incorrecto:

```
classname      = com.ibm.iop.cat.fw.remote.IopCatRemoter
0050.rhosturl      = https://${APP_HOSTNAME_1}:9443/IopCatRemoteResponder/IopCatRemoteResponder
0050.remoteclassname= com.ibm.iop.cat.fw.Echo
0050.displaylabel   = Internal Diagnostic (Echo REST remoted)
0050.comment        = Self diagnostic CAT check. Tests link between to CAT modules.
0050.failinfopage   = cct_echo_rest_remoted_test.html
```

Should be:

```
0050.classname      = com.ibm.iop.cat.fw.remote.IopCatRemoter
0050.rhosturl       = https://${APP_HOSTNAME_1}:9443/IopCatRemoteResponder/IopCatRemoteResponder
0050.remoteclassname= com.ibm.iop.cat.fw.Echo
0050.displaylabel   = Internal Diagnostic (Echo REST remoted)
0050.comment        = Self diagnostic CAT check. Tests link between to CAT modules.
0050.failinfopage   = cct_echo_rest_remoted_test.html
```

CIYBA0345E Clave no válida: el prefijo de la clave no es numérico. Parámetros: {0}: nombre de clase {1}: nombre de método {2}: número de secuencia CCT_RESULTS_INFO = {0}.{1}() - Clase: {2} Resultados - Código de respuesta[{3}] Texto de respuesta[{4}]

Explicación: Cada prueba debe tener un prefijo numérico que agrupe todas las propiedades de una prueba determinada. El prefijo proporcionado no es numérico.

Respuesta del Usuario: Busque el número de secuencia en el archivo de propiedades. Cambie el prefijo a numérico y use el mismo para el resto de propiedades de la prueba.

CIYBA0347E Se ha producido una excepción. Parámetros: {0}: nombre de clase {1}: nombre de método {2}: cadena de excepción

Explicación: Se ha producido una excepción.

Respuesta del Usuario: Examine la cadena de excepción para determinar la causa del error de la prueba. Es posible que sea un error de prueba normal. Por ejemplo, "Conexión rechazada" suele significar que ningún programa escuchaba en el puerto y que el servicio no se está ejecutando.

CIYBA0348E Se ha pulsado un botón para ejecutar una prueba, pero no se han encontrado propiedades coincidentes en el archivo de propiedades.

Explicación: No se han encontrado propiedades para la prueba. Es posible que el archivo de propiedades haya cambiado.

Respuesta del Usuario: Pulse **Restablecer**. Se volverá a cargar el archivo de propiedades actual.

CIYBA0349E El código especificado por la clase no se ha encontrado. Parámetro:{0}: nombre de clase (no encontrado)

Explicación: O bien `classname` no se ha especificado correctamente en el archivo de propiedades o el código no se ha encontrado.

Respuesta del Usuario: Compruebe las bibliotecas compartidas de `IopCatRemoteResponder` para consultar si falta alguna.

CIYBA0401E El nombre del archivo de la plantilla de propiedades IOPMGMT no se ha especificado o es incorrecto.

Explicación: Falta el parámetro del archivo de la plantilla de propiedades IOPMGMT.

Respuesta del Usuario: Introduzca el nombre correcto del archivo de propiedades IOPMGMT.

CIYBA0402E El nombre del archivo de propiedades de topología no se ha especificado o es incorrecto.

Explicación: Falta el parámetro del archivo de propiedades de topología o es incorrecto.

Respuesta del Usuario: Introduzca el nombre correcto del archivo de propiedades de topología.

CIYBA0403E El nombre del archivo de la plantilla de propiedades IOPMGMT no se ha especificado o es incorrecto.

Explicación: Falta el parámetro que especifique el archivo de la plantilla de propiedades IOPMGMT.

Respuesta del Usuario: Introduzca el nombre del archivo correcto para el archivo de propiedades de topología.

CIYBA0404E El archivo de propiedades de topología no se encuentra.

Explicación: El archivo de propiedades de topología no se encuentra.

Respuesta del Usuario: Compruebe que el archivo de propiedades de topología esté en el directorio *inicio_instalación*`/topology` de servidor de instalación.

CIYBA0405E Falta la contraseña en el archivo de topología de la propiedad:

Explicación: No se ha encontrado ninguna contraseña en el archivo de propiedades de topología indicado.

Respuesta del Usuario: Se necesita una contraseña para el archivo de topología. Introduzca una contraseña para la topología.

CIYBA0501E Falta el parámetro necesario para Base Architecture Cyber Hygiene Media.

Explicación: Falta el parámetro necesario para IBM Intelligent Operations Center Cyber Hygiene Media.

Respuesta del Usuario: Compruebe que la vía de acceso del script de Cyber Hygiene a la ubicación del soporte de instalación sea correcta.

CIYBA0502E Falta el parámetro necesario para el archivo de propiedades de topología.

Explicación: Falta el parámetro del nombre de archivo del archivo de propiedades de topología.

Respuesta del Usuario: Introduzca el nombre del archivo correcto para el archivo de propiedades de topología.

CIYBA0503E Falta el parámetro necesario para el directorio de destino de Base Architecture Cyber Hygiene.

Explicación: Falta el parámetro necesario para el directorio de destino de Cyber Hygiene.

Respuesta del Usuario: Proporcione el directorio de destino correcto.

CIYCC0002E Corrija los siguientes errores de configuración: {0}

Explicación: Se ha producido un error en la página de configuración Editar sesiones compartidas. El error se indica mediante {0}.

Respuesta del Usuario: Corrija el error y vuelva a intentar la solicitud.

CIYCC0005E No se puede enviar el suceso. Intente enviar el suceso de nuevo. Si el problema continúa, póngase en contacto con el administrador o con el servicio de asistencia técnica.

Explicación: Se ha producido un error de servlet de publicación cuando un usuario intentaba actualizar, escalar o cancelar un suceso.

Respuesta del Usuario: Solicite al administrador o al servicio de asistencia técnica que resuelva el error de servlet de la publicación.

CIYCC0006W Otro usuario ha actualizado el registro. Renueve la página para alcanzar el registro actualizado.

Explicación: Una actualización solicitada por el usuario ha entrado en conflicto con otro cambio producido en el servidor. Esto puede ocurrir cuando dos usuarios intentan cambiar el estado de una actividad a la vez.

Respuesta del Usuario: Renueve la página. Se mostrará la actualización realizada por el otro usuario. A continuación, aplique los cambios necesarios.

CIYUI0001E La matriz JSON proporcionada contiene errores y no se puede analizar.

Explicación: El usuario ha introducido una cadena JSON en una ventana donde se debe introducir el script, pero la cadena contiene errores de sintaxis y no se puede analizar.

Respuesta del Usuario: Corrija la cadena JSON.

CIYUI0002E No se ha encontrado el suceso. No se pueden mostrar las propiedades del suceso.

Explicación: La solicitud para mostrar las propiedades del suceso ha fallado porque no se han encontrado propiedades en la base de datos.

Respuesta del Usuario: Renueve la página y vuelva a intentar la solicitud.

CIYUI0004E Error de envío de datos de gestor de mapa de ubicación.

Explicación: Se ha producido un problema al establecer los datos del gestor de mapa de ubicación.

Respuesta del Usuario: Consulte los mensajes adicionales para obtener más detalles.

Mensajes adicionales de la pestaña Clasificaciones.

Error de envío de datos
La nueva clasificación no se ha introducido en la base de datos.

Mensajes adicionales de la pestaña Mapas de ubicación.

Error de envío de datos
El nuevo mapa de ubicación no se ha introducido en la base de datos.

Mensajes adicionales de la pestaña Áreas.

El identificador de área introducido no es válido. El identificador de área ya existe en el mapa.
El usuario está entrando en un área del mapa que ya existe en el mapa.

El identificador de área introducido no es válido.
El identificador de área no es válido. O bien está vacío o el ID de área es igual al ID del área padre.

Los datos de área introducidos no son válidos.
Los datos de área no son válidos. El cliente debe comprobar que ha introducido todos los campos necesarios para cada área.

El identificador de área padre no existe como área en el mapa actual.
El ID de área padre introducido existe como área en el mapa. Un área no puede tener un área padre que sea un área del mapa. Debe estar en otro mapa.

Hay referencias circulares entre las áreas y sus áreas principales. Elimine las referencias circulares.
Elimine las relaciones del área padre circular de la base de datos IBM Intelligent Operations Center.

Error de envío de datos.
La nueva pestaña de áreas no se ha introducido en la base de datos.

CIYUI0003I Los datos se enviaron con éxito.

Explicación: Este mensaje solo tiene fines informativos. El mensaje indica que la base de datos deIBM Intelligent Operations Center, el portlet Gestor de mapas de ubicación y e l portlet Mapa de ubicación se han actualizado.

Respuesta del Usuario: No es necesaria ninguna acción.

CIYUI0004I Enviado con éxito.

Explicación: Este mensaje solo tiene fines informativos. El mensaje indica que solo se ha actualizado la IU del portletGestor de mapas de ubicación, los cambios no se han almacenado en la base de datos deIBM Intelligent Operations Center. Si sale del portlet Gestor de mapas de ubicación sin enviar los cambios, la actualización se cancelará.

Respuesta del Usuario: Haga clic en **Enviar** para actualizar la base de datos de IBM Intelligent Operations Center y el portlet Mapa de ubicación.

Uso de las bases de conocimiento y de IBM Support

Esta sección contiene temas para el uso de las bases de conocimiento, Fix Central e IBM Support para buscar soluciones a sus problemas.

Búsqueda en bases de conocimiento

A menudo puede encontrar la solución al problema realizando búsquedas en las bases de conocimiento de IBM. Puede optimizar los resultados mediante los recursos, las herramientas de soporte y los métodos de búsqueda disponibles.

Acerca de esta tarea

Puede encontrar información útil buscando en el Information Center para IBM Intelligent Operations Center, pero algunas veces necesita mirar más allá del Information Center para responder a sus preguntas o resolver problemas.

Procedimiento

Para buscar la información que necesita en las bases de conocimientos, utilice uno o más de los siguientes métodos:

- Busque contenido utilizando IBM Support Assistant Lite (ISA Lite).

  ISA Lite es una herramienta de software sin cargo que le ayuda a resolver dudas y problemas relacionados con productos de software IBM. Para obtener instrucciones sobre cómo descargar e instalar ISA Lite, consulte los enlaces al final del tema.
- Busque el contenido que necesita utilizando elPortal de soporte de IBM.

  El portal de soporte técnico de IBM es una vista centralizada y única de toda la información y las herramientas de soporte técnico para todos los servicios, el software y los sistemas de IBM. El portal de soporte de IBM le permite acceder a la cartera de soporte electrónico de IBM desde un sitio. Puede adaptar las páginas para centrarse en la información y los recursos que necesite para prevenir problemas y resolverlos con mayor rapidez. Familiarícese con el portal de soporte de IBM visualizando los vídeos de demostración (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) de esta herramienta. Estos vídeos constituyen una presentación del portal de soporte de IBM, exploran el entorno de la resolución de problemas y otros recursos, y demuestran de qué manera puede adaptar la página moviendo, añadiendo y suprimiendo portlets.
- Busque el contenido acerca de IBM Intelligent Operations Center mediante el uso de uno de los siguientes recursos técnicos adicionales:
  - IBM Intelligent Operations Center notas técnicas y APAR (informes de problemas)
  - Página del portal de soporte de IBM Intelligent Operations Center
  - Páginas de foros y comunidades de IBM Intelligent Operations Center
  - IBM Smarter Cities Software Solutions Redbooks
- Busque contenido utilizando la búsqueda de cabecera de IBM. Puede utilizar la búsqueda de cabecera de IBM tecleando su serie de búsqueda en el campo Buscar en la parte superior de cualquier página de ibm.com.
- Busque contenido utilizando un motor de búsqueda externo como, por ejemplo, Google, Yahoo o Bing. Si utiliza un motor de búsqueda externo, es más probable que los resultados incluyan información que

esté fuera del dominio ibm.com. Sin embargo, a veces puede encontrar información útil sobre resolución de problemas de productos de IBM en grupos de noticias, foros y blogs que no están en ibm.com.

Consejo: Incluya "IBM" y el nombre del producto en la búsqueda si busca información sobre un producto de IBM.

Conceptos relacionados:

"Acerca de" en la página 199
Utilice el portlet Acerca de para ver detalles de la versión del IBM Intelligent Operations Center y el IBM Smarter Cities Software Solutions integrado que ha instalado. También puede ver detalles de las actualizaciones que aplicó desde la instalación.

"Instalación y utilización de IBM Support Assistant Lite" en la página 310
IBM Support Assistant Lite (ISA Lite) es una herramienta que recopila datos comunes de diagnóstico que son útiles para analizar problemas generales.

Información relacionada:

Descargando IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5

Obtención de arreglos de Fix Central

Puede utilizar Fix Central para buscar los arreglos recomendados por el servicio de soporte de IBM para varios productos, incluyendo IBM Intelligent Operations Center. Con Fix Central, puede buscar, seleccionar, solicitar y descargar arreglos para su sistema con una amplia gama de opciones de entrega. Es posible que haya disponible un arreglo del producto IBM Intelligent Operations Center para resolver el problema.

Procedimiento

Para buscar e instalar arreglos:

1. Consiga las herramientas necesarias para obtener el arreglo. Si no está instalado, consiga el instalador de actualización de su producto. Puede descargar el instalador de Fix Central. Este sitio ofrece instrucciones de descarga, instalación y configuración para el instalador de actualización.
2. Seleccione el producto IBM Intelligent Operations Center y después seleccione los recuadros de selección que estén relacionados con su problema.
3. Identifique y seleccione el arreglo que necesita.
4. Descargue el arreglo.
   a. Abra el documento de descarga y siga el enlace de la sección "Paquete de descarga".
   b. Al descargar el archivo, asegúrese de que no se cambia el nombre del archivo de mantenimiento. Este cambio podría ser intencionado o puede que sea un cambio involuntario causado por determinados navegadores web o programas de utilidad de descarga.
5. Para aplicar el archivo, siga las instrucciones de la sección "Instrucciones de instalación" del documento de descarga.
6. Opcional: Suscríbase para recibir notificaciones de correo electrónico semanales sobre arreglos y otras actualizaciones del servicio de soporte de IBM.

Tareas relacionadas:

"Suscripción a actualizaciones de soporte" en la página 333
Para mantenerse informado de las noticias más importantes sobre los productos de IBM que utiliza, suscríbase a las actualizaciones.

Información relacionada:

Ayuda de Fix Central

Contacto con el soporte delIBM

IBM Support ofrece asistencia para resolver defectos de producto, responder preguntas frecuentes y realizar redescubrimientos.

Antes de empezar

Tras intentar encontrar una respuesta o una solución utilizando otras opciones de autoayuda, como las notas técnicas, puede ponerse en contacto con el soporte de IBM. Antes de ponerse en contacto con el Soporte técnico de IBM, su empresa debe tener un contrato de suscripción de software y de soporte técnico de IBM activo, y usted debe estar autorizado para enviar problemas a IBM. Para obtener información sobre los tipos de soporte disponibles, consulte el tema Support portfolio de la publicación *Software Support Handbook*.

Procedimiento

Complete los pasos siguientes para ponerse en contacto con IBM Support con un problema:

1. Defina el problema, especifique el contexto y determine la gravedad del problema. Para obtener más información, consulte el tema Getting IBM support (Obtención de soporte de IBM) del manual *Software Support Handbook*.
2. Recopile información de diagnóstico. Para obtener información sobre el uso de IBM Support Assistant Lite para recopilar los archivos de registro de IBM Intelligent Operations Center, consulte los enlaces al final del tema.
3. Envíe el problema al servicio de soporte de IBM de una de las maneras siguientes:
   - Utilizando IBM Support Assistant Lite (ISA Lite). Consulte los enlaces al final del tema.
   - En línea a través de Página del portal de soporte de IBM Intelligent Operations Center : Puede abrir, actualizar y ver todas las solicitudes de servicio del portlet de solicitud de servicio en la página de solicitud de servicio.
   - Por teléfono: Por el número de teléfono para llamar en su región, consulte la página web del Directorio de contactos en todo el mundo .

Resultados

Si el problema que envía es relativo a un defecto de software o a una documentación imprecisa o ausente, el Soporte técnico de IBM crea un informe autorizado de análisis de programa (APAR). El APAR describe el problema en detalle. Siempre que sea posible, el soporte de IBM proporcionará una solución que podrá implementar hasta que el APAR se resuelva y se proporcione un arreglo. IBM publica diariamente los APAR resueltos en el sitio web de soporte de IBM, para que otros usuarios que tienen el mismo problema puedan beneficiarse de la misma resolución.

Qué hacer a continuación

Esté preparado para trabajar con el representante de soporte técnico de IBM mediante la Asistencia en el sitio de IBM, que es un plug-in de asistencia remota que puede descargar a su sistema. El representante de soporte técnico de IBM puede utilizar IBM Assist On-Site para ver su escritorio y compartir el control del ratón y el teclado. Esta herramienta acorta el tiempo que se tarda en identificar el problema, recopilar los datos necesarios y solucionar el problema. Para obtener más información, consulte IBM Assist On-Site.

Conceptos relacionados:

"Acerca de" en la página 199
Utilice el portlet Acerca de para ver detalles de la versión del IBM Intelligent Operations Center y el IBM Smarter Cities Software Solutions integrado que ha instalado. También puede ver detalles de las actualizaciones que aplicó desde la instalación.

"Instalación y utilización de IBM Support Assistant Lite" en la página 310
IBM Support Assistant Lite (ISA Lite) es una herramienta que recopila datos comunes de diagnóstico que son útiles para analizar problemas generales.

Información relacionada:

Descargando IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5

Suscripción a actualizaciones de soporte

Para mantenerse informado de las noticias más importantes sobre los productos de IBM que utiliza, suscríbase a las actualizaciones.

Acerca de esta tarea

Al suscribirse para recibir actualizaciones, puede recibir importante información técnica y actualizaciones para herramientas y recursos de IBM concretas.Puede suscribirse a actualizaciones de dos formas:

canales de información RSS
La siguiente fuente RSS está disponible para IBM Intelligent Operations Center: *IBM Intelligent Operations Center*.

Para obtener información general sobre RSS, incluyendo los pasos para empezar y una lista de las páginas web de IBM con RSS habilitado, visite el sitioCanales de información RSS de soporte de software de IBM.

Mis Notificaciones
Con Mis notificaciones, puede suscribirse a las actualizaciones de soporte de cualquier producto de IBM. (Mis notificaciones sustituye a Mi soporte, una herramienta similar que quizás haya utilizado en el pasado.) Con Mis notificaciones, puede especificar que desea recibir anuncios semanales o diarios por correo electrónico. Puede especificar qué tipo de información desea recibir (como por ejemplo publicaciones, consejos y sugerencias, flashes de producto (también conocidos como alertas), descargas y controladores). Mis notificaciones le permite personalizar y clasificar los productos sobre los que desea mantenerse informado y los métodos de entrega que mejor se adaptan a sus necesidades.

Procedimiento

Para suscribirse a las actualizaciones de soporte:

1. Para subscribirse a la fuente RSS de *IBM Intelligent Operations Center* , utilice los siguientes subpasos:
   a. Abra el enlace Canal de información RSS de IBM Intelligent Operations Center .
   b. En la ventana Suscribirse a Live Bookmark , seleccione una carpeta en la que guardar el marcador de fuentes RSS y pulse **Suscribir**.

   Para obtener más información sobre la suscripción a fuentes RSS, consulte el enlace de fuentes RSS del Soporte de software de IBM en la sección Información relacionada al final del tema.
2. Para suscribirse a Mis notificaciones, vaya a IBM Support Portal y pulse **Mis notificaciones** en el portlet **Notificaciones**.
3. Regístrese utilizando su ID de usuario y contraseña de IBM, y pulse en **Submit**.
4. Identifique qué y cómo desea recibir las actualizaciones.
   a. Pulse la pestaña **Suscribirse**.
   b. Seleccione IBM Intelligent Operations Center y pulse **Continuar**.

c. Seleccione sus preferencias acerca de cómo recibir actualizaciones, ya sea por correo electrónico, en línea en una carpeta designada o por medio de un canal de información RSS o Atom.
d. Seleccione los tipos de actualizaciones de documentación que desee recibir, por ejemplo, información nueva sobre descargas del producto y comentarios de los grupos de discusión.
e. Pulse **Enviar**.

Resultados

Hasta que modifique su canal de información RSS y las preferencias de Mis notificaciones, recibirá las notificaciones o las actualizaciones que haya solicitado. Puede modificar las preferencias cuando sea necesario (por ejemplo, si deja de utilizar un producto y empieza a utilizar otro).

Tareas relacionadas:

"Obtención de arreglos de Fix Central" en la página 331
Puede utilizar Fix Central para buscar los arreglos recomendados por el servicio de soporte de IBM para varios productos, incluyendo IBM Intelligent Operations Center. Con Fix Central, puede buscar, seleccionar, solicitar y descargar arreglos para su sistema con una amplia gama de opciones de entrega. Es posible que haya disponible un arreglo del producto IBM Intelligent Operations Center para resolver el problema.

Información relacionada

Canales de información RSS de Soporte de software de IBM

Suscribirse a las actualizaciones de contenido de soporte de Mis notificaciones

Mis notificaciones para el soporte técnico de IBM

Mis notificaciones para información general de soporte técnico de IBM

Intercambio de información con IBM

Para diagnosticar o identificar un problema, es posible que tenga que proporcionar al servicio de soporte de IBM datos e información sobre el sistema. En otros casos, el servicio de soporte de IBM le proporcionará herramientas o programas de utilidad que utilizar para la determinación de problemas.

Conceptos relacionados:

"Habilitación de seguimientos y visualización de archivos de registros" en la página 301
Para solucionar un problema en IBM Intelligent Operations Center , es posible que tenga que analizar los archivos de registro en varios sistemas. Los siguientes temas le proporcionan orientación sobre cómo acceder a los archivos de registro.

"Instalación y utilización de IBM Support Assistant Lite" en la página 310
IBM Support Assistant Lite (ISA Lite) es una herramienta que recopila datos comunes de diagnóstico que son útiles para analizar problemas generales.

Tareas relacionadas:

"La ejecución de la instalación debe reunir la herramienta" en la página 305
Los archivos de registro se generan mientras se está instalando IBM Intelligent Operations Center . Hay una herramienta para recopilar estos archivos de registro para su análisis.

Información relacionada:

Descargando IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5

Envío de información al soporte de IBM

Para reducir el tiempo que se tarda en resolver un problema, puede enviar información de rastreo y de diagnóstico a IBM Support.

Procedimiento

Para enviar información de diagnóstico al soporte de IBM:

1. Abra un registro de gestión de problemas (PMR) utilizando la herramienta de solicitud de servicio.
2. Recopile los datos de diagnóstico que necesite. Los datos de diagnóstico ayudan a reducir el tiempo que se tarda en resolver el PMR. Puede recopilar los datos de diagnóstico automática o manualmente:
   - Recopile los datos de forma automática utilizando IBM Support Assistant Lite (ISA Lite). Consulte los enlaces situados al principio del tema.
   - Recopilar los datos manualmente. Para obtener información acerca de los archivos de registro IBM Intelligent Operations Center , consulte los enlaces cerca del comienzo del tema.
3. Comprima los archivos utilizando el formato ZIP o TAR.
4. Transfiera los archivos a IBM. Puede utilizar uno de los métodos siguientes para transferir los archivos a IBM:
   - La herramienta de solicitud de servicio
   - Métodos estándar de carga de datos: FTP, HTTP
   - Métodos seguros de carga de datos: FTPS, SFTP, HTTPS
   - Correo electrónico

   Todos estos métodos de intercambio de datos se explican en el sitioIBM Support.

Recepción de información del soporte de IBM

En ocasiones, es posible que un representante del soporte técnico de IBM le pida que descargue herramientas de diagnóstico u otros archivos. Puede usar el FTP para descargar estos archivos.

Antes de empezar

Asegúrese de que su representante de soporte técnico de IBM le haya proporcionado el servidor preferido que debe usar para descargar los archivos, además de los nombres exactos de archivo y directorio a los que acceder.

Procedimiento

Para descargar archivos del servicio de soporte de IBM:

1. Utilice FTP para conectar con el sitio que el representante del servicio de soporte técnico de IBM le haya indicado e inicie sesión como usuario `anonymous`. Utilice su dirección de correo electrónico como contraseña.
2. Vaya al directorio que corresponda:
   a. Vaya al directorio `/fromibm`.
      ```
      cd fromibm
      ```
   b. Vaya al directorio proporcionado por su representante de soporte técnico de IBM.
      ```
      cd nombre_directorio
      ```
3. Habilite la modalidad binaria para su sesión.
   ```
   binary
   ```
4. Utilice el mandato **get** para descargar el archivo especificado por el representante de soporte técnico de IBM.
   ```
   get nombre_archivo.extensión
   ```
5. Finalice la sesión de FTP.
   ```
   quit
   ```

Problemas conocidos y soluciones

Esta sección contiene una lista de los problemas que se producen con más frecuencia y una solución para cada elemento.

El proceso del indicador clave de rendimiento se detiene después de un periodo

En IBM Intelligent Operations Center, el proceso del indicador clave de rendimiento (KPI) se detiene ocasionalmente después de un periodo por ejemplo, de noche. Para obtener información acerca de la resolución del problema, consulte el enlace al final del tema para la nota técnica de resolución de problemas *El proceso del indicador clave de rendimiento se detiene después de un periodo de tiempo* .

Portlets no llenos de datos cuando cambia la configuración de seguridad

Si los portlets no se llenan con KPI, datos de actividad o de recurso tal como esperaba, compruebe la configuración del puerto. Si utiliza tabla de propiedades del sistema para cambiar la configuración de HTTPS y no cambia la configuración del puerto en consecuencia, se producirá un problema al llenar los portlets con datos.

Error de conexión de informe Cognos

Si recibe un error de conexión de informe Cognos , renueve la página.

Los informes de Cognos no se muestran correctamente

Si los informes de Cognos no se muestran correctamente al abrir la página de Supervisor: informes o Operador: informes, renueve la página.

Si tras renovar la página, los informes de Cognos siguen sin mostrarse correctamente, quizá se deban detener los clústers del servidor de aplicaciones de Cognos. Inicie sesión en la consola de administración de WebSphere Application Server y compruebe el estado de los clústers deWebSphere Application Server. Si en el estado de alguno de los clústers se muestra una X en rojo, seleccione dicho clúster y pulse**Inicio**.

No se encuentran datos para los informes de Cognos

Si los informes de Cognos no se muestran correctamente y recibe el mensaje `No se encuentran datos`, puede que no existan datos con los criterios de selección en la base de datos. Redefina dichos criterios de selección. Por ejemplo, elimine los campos **Desde** y**Hasta** en el informe personalizado y haga clic en**Actualizar**. A continuación, copie el URL del informe y péguelo en el portletCognos.

El informe no se muestra cuando se copia la URL del informe utilizando el botón URL de informe

Como usuario de muestra, si copia la dirección URL del informe utilizando el botón **URL de informe** y, a continuación, va directamente a la página Portlet de informes, el informe no se muestra. Para arreglar este problema, pulse **F5** para actualizar y que el informe se muestre correctamente.

El recurso editado no se muestra en el portlet de Detalles

Si edita un recurso en Tivoli Service Request Manager mientras Tivoli Netcool/Impact no está disponible, es posible que el recurso no se muestre en el portlet Detalles . Por ejemplo, si pulsa con el botón derecho del ratón sobre un suceso en la pestaña **Sucesos e incidentes** y, a continuación, pulsa **Ver recursos de la zona**, es posible que el recurso editado no se muestre. Para resolver el problema, edite el recurso de nuevo en Tivoli Service Request Manager.

El estado de usuarios que han cerrado sesión no se muestra correctamente en el portlet Contactos

El estado de los usuarios que han iniciado sesión se visualiza en el portlet Contactos. Si un usuario que ha iniciado sesión cierra la ventana del navegador o finaliza la sesión en WebSphere Portal, el estado de dicho usuario todavía se visualiza como conectado hasta que la sesión caduque. Sin embargo, los mensajes que se envían a este usuario, después de que el usuario haya cerrado la ventana del navegador o finalizado la sesión, no se entregan. Por lo tanto, se muestra un mensaje de error al usuario que intenta enviar el mensaje. Para asegurarse de que el estado se actualice de inmediato en el portlet Contactos, cierre sesión pulsando **Archivo** > **Finalizar sesión**.

Selección de Actualizar más de uno en la página Informes de supervisor

En la página Supervisor: Informes de la interfaz de usuario de IBM Intelligent Operations Center, al seleccionar **Actualizar** sin realizar cambios, los campos **Desde la fecha** y **Hasta la fecha** se llenarán con la fecha actual. Si selecciona **Actualizar** de nuevo sin realizar cambios, se mostrará el mensaje `No se encontraron datos`.

Este comportamiento ocurre porque los campos **Desde la fecha** y **Hasta la fecha** se llenan de forma automática.

Los titulares demasiado largos inutilizan los gráficos de informes

Los titulares de sucesos que superan los 20-30 caracteres pueden afectar al modo en que se muestra el informe de gráfico circular **Todos los sucesos, por titular**, inutilizándolo. Los titulares de suceso etiquetan las secciones del gráfico circular y éste se reduce para adaptarse a las etiquetas, por tanto, la imagen del gráfico circular se muestra demasiado pequeña para distinguirse entre las diferentes secciones.

Resultados inesperados en la conversión de la zona horaria del navegador

Unos resultados inesperados en la conversión de la zona horaria del navegador podrían deberse a una codificación de zona horaria incorrecta en el suceso Common Alerting Protocol (CAP). Para obtener más información, consulte el enlace al final del tema.

Conceptos relacionados:

"Utilización del PAC para sucesos de ICR" en la página 100
El WebSphere Message Broker, que se proporciona como parte de IBM Intelligent Operations Center, acepta mensajes de suceso CAP y utiliza los datos en los cálculos del indicador clave de rendimiento (KPI) .

Información relacionada:


El proceso del indicador clave de rendimiento se detiene después de un periodo de tiempo resolviendo problemas de notas técnicas

Errores de conexión al instalar IBM Intelligent Operations Center

Qué se debe hacer cuando se emite un mensaje SOAPException al instalar IBM Intelligent Operations Center.

Si se emite un mensaje como el siguiente significa que la conexión con un servidor se ha perdido:

```
[SOAPException: faultCode=SOAP-ENV:Client; msg=Read timed out
```

Si esto ocurre, detenga y reinicie los servidores. A continuación, reinicie el instalador o vuelva a ejecutar el mandato de instalación.

La red IPv6 no se inicia

Si la red IPv6 no se inicia en un servidor, es posible que el archivo `/etc/modprobe.conf` requiera cambios.

Acerca de esta tarea

Este problema se produce al actualizar VMWare al release 5.

Procedimiento

1. Edite el archivo `/etc/modprobe.conf` .
2. Cambie a la siguiente línea:

   ```
   alias ipv6 off
   ```

   en

   ```
   # alias ipv6 off
   ```
3. Cambie a la siguiente línea:

   ```
   options ipv6 disable=1
   ```

   en

   ```
   # options ipv6 disable=1
   ```
4. Guarde el archivo.
5. Vuelva a iniciar el servidor.

Tivoli Service Request Manager no se inicia

Qué se debe hacer si Tivoli Service Request Manager no se puede iniciar mediante Herramienta de control de plataforma y la herramienta Comprobación de verificación del sistema lo muestra como si funcionase.

Acerca de esta tarea

Para reiniciar Tivoli Service Request Manager, realice las siguientes acciones.

Procedimiento

1. Detenga todos los servicios utilizando Herramienta de control de plataforma.
2. Cierre y reinicie servidor de sucesos.
3. Inicie todos los servicios utilizando Herramienta de control de plataforma.

No se puede crear una página nueva para la interfaz de usuario

Resuelva los problemas relacionados con la creación de una página nueva si trabaja conMicrosoft Internet Explorer 9.

Acerca de esta tarea

Este problema puede producirse al intentar crear una página nueva a partir de la página **Administración** o cualquiera de las páginas de usuario de **Citywide**. La página nueva no se carga. Para acabar con el problema, cambie el navegador a**Vista de compatibilidad** temporalmente. Debe asegurarse de que desactiva la **Vista de compatibilidad** tras haber creado la página nueva, ya queIBM Intelligent Operations Center no soporta la Vista de compatibilidad de Internet Explorer 8 o Internet Explorer 9.

Procedimiento

1. Abra Internet Explorer 9.
2. Inicie sesión en IBM Intelligent Operations Center como administrador.

3. Haga clic en **Administración** > **Interfaz de usuario del portal** > **Gestionar páginas**.
4. En la barra de herramientas superior del navegador, haga clic en **Herramientas**.
5. En el menú, seleccione **Vista de compatibilidad**.
6. Escriba `citywide` en el cuadro de búsqueda.
7. Cuando termine la búsqueda, haga clic en **citywide**.
8. Haga clic en **Página nueva**.
9. Cuando se cargue la página nueva, vuelva a la barra de herramientas del navegador y anule la selección de **Vista de compatibilidad**.

Conceptos relacionados:

"Navegadores compatibles" en la página 13
La interfaz de soluciones de IBM Intelligent Operations Center soporta varios navegadores. Algunos navegadores pueden utilizarse con limitaciones.

Soluciones temporales de accesibilidad para portlets

Existen soluciones temporales para problemas de accesibilidad que se relacionan con algunos de los portlets de IBM Intelligent Operations Center :

- En el portlet Detalles y el portlet Notificaciones , para acceder al menú emergente, utilice los siguientes controles de teclado:

  Windows
  Pulse la tecla del menú dedicado.

  Mac Elija la opción adecuada dependiendo de si tiene un teclado numérico:
  - Si tiene un teclado numérico, asegúrese de que las teclas del ratón están habilitadas y, a continuación, pulse Control+5.
  - Si no tiene teclado numérico, habilite las teclas de ratón y, a continuación, pulse Control+I.

- Para abrir la ventana Añadir suceso , en el portlet Detalles , pulse la pestaña **Sucesos e incidencias** , o pulse la tecla Tab, el lector de pantalla lee los nombres de las pestañas. Después, seleccione los controles de teclado adecuados de la lista.

  Mozilla Firefox
  Control+Alt+V

  Safari fn+control+opción+V

  Internet Explorer
  Control+Alt+V

- En el portlet Detalles , en la ventana Añadir suceso , el lector de pantalla no lee los siguientes valores:
  - **Fecha efectiva**
  - **>Hora efectiva**
  - **Fecha de comienzo**
  - **Hora de comienzo**
  - **Fecha de caducidad**
  - **Hora de caducidad**

Método alternativo de accesibilidad para seleccionar fechas en el portlet Informes

En el portlet Informes, no se pueden seleccionar las fechas del calendario a través del teclado.

Acerca de esta tarea

En el portlet Informes, para configurar un informe predefinido, debe introducir una fecha o un rango de fechas. Sin embargo, no se puede acceder al selector de fechas del calendario a través del teclado. Se muestra el calendario, pero no puede seleccionar una fecha desde el calendario utilizando el teclado. Seleccionar fechas desde el calendario sólo funciona si utiliza un ratón.

Para una solución para este problema, complete los pasos siguientes para entrar las fechas manualmente utilizando el teclado.

Procedimiento

1. En el portlet Informes, seleccione el informe predefinido en la parte inferior de la página y pulse **Configurar el informe** .
2. En el campo **Desde la fecha** , entre la fecha para la que está visualizando la información. Si está entrando un rango de fecha, esta fecha es la fecha de inicio.
3. En el campo **Hasta la fecha** , entre la última fecha en el rango de fechas para la información del informe.
4. Pulse **Ver el informe**.

Los sucesos nuevos no se muestran actividades en el portlet Detalles

Si los sucesos nuevos no se muestran actividades en el portlet Detalles, siga los pasos indicados a continuación para resolver el problema.

Acerca de esta tarea

Si el primer paso no resuelve el problema, continúe con el paso siguiente. Siga todos los pasos hasta que el problema se haya resuelto.

Procedimiento

1. Compruebe el estado del analizador XML de IBM Intelligent Operations Center
   a. Inicie sesión en el servidor de sucesos como `root` y escriba el siguiente mandato:
      ```
      – tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
      ```
   b. Compruebe que se muestra `Connection status OK` en la parte inferior del archivo.
   c. Si se muestra el mensaje `Probe shutting down` o si la fecha/hora no coincide con la hora actual del servidor, complete los pasos siguientes:
      1) Cambie el nombre al registro actual escribiendo el siguiente mandato:
         ```
         - mv /opt/IBM/netcool/omnibus/log/ioc_xml.log
         /opt/IBM/netcool/omnibus/log/old_ioc_xml.log
         ```
      2) Reinicie el analizador escribiendo el siguiente mandato:
         ```
         /opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile
         /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
         ```
      3) Espere aproximadamente 1 minuto y escriba el siguiente mandato:
         ```
         – tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
         ```
         Busque el mensaje `Connection Status OK`. Si el estado de conexión no es correcto, busque errores en el archivo. Los problemas de conexión pueden indicar que el servidor de objetos no está activo. Consulte el paso 2.
2. Si el analizador XML de IBM Intelligent Operations Center continúa apagado, complete los pasos indicados a continuación para comprobar el estado de la base de datos de Tivoli Netcool/OMNIbus. Si el analizador XML de IBM Intelligent Operations Center no continúa apagado, vaya al paso3 en la página 341.
   a. Inicie sesión en el servidor de sucesos como `ibmadmin` y escriba el siguiente mandato:

```
- /opt/IBM/netcool/omnibus/bin/nco_config &
```

b. Si se le pregunta si desea realizar la importación de `omni.dat`, seleccione **Sí** y haga clic en **Finalizar**.

c. Minimice la ventana del agente de procesos y pulse con el botón derecho **NCOMS**.

Si la opción **Conectar como** está disponible, haga clic en ella y conéctese como `raíz` utilizando la contraseña de topología.

Si no ve la opción **Conectar como**, cierre `nco_config` y como `ibmadmin`, escriba el mandato siguiente para iniciar el servidor de objetos NCOMS:

```
- /opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &
```

Si el servidor de objetos NCOMS no se inicia, abra `/opt/IBM/netcool/omnibus/var`, localice y elimine el archivo `NCOMS.pid`, y escriba el mandato siguiente:

```
/opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &
```

Nota: Tras iniciar el servidor de objetos NCOMS, debe reiniciar el analizador XML IBM Intelligent Operations Center. Vea el paso 1 en la página 340.

3. Compruebe el estado de Tivoli Netcool/Impact.

a. Inicie sesión en el servidor de sucesos en http://*EventsHost*:9080/nci/login_main.jsp como `admin`.

Si no puede iniciar sesión, ejecute los mandatos siguientes en el servidor de sucesos:

```
su – netcool
/opt/IBM/netcool/bin/ewas.sh start
```

b. En la ventana **Estado de servicio**, desplácese hacia abajo y asegúrese de que se están ejecutando los siguientes servicio:

- **EventProcessor**
- **IOC_CAP_Event_Reader**
- **IOC_Notification_Reader**

Nota: Junto a los servicios en ejecución se mostrará un signo de verificación verde.

c. En la ventana **Estado de servicio**, haga clic con el icono **Ver registro** situado junto a **PolicyLogger**, y busque errores en el archivo de registro.

Si encuentra errores en el registro, puede ver los detalles del archivo de registro en `/opt/IBM/netcool/impact/log/`. Para conocer más detalles, haga clic en **PolicyLogger**, defina el **Nivel de registro superior** en**3** y seleccione las casillas de verificación relevantes.

4. Compruebe si existen sucesos bloqueados en las colas de WebSphere MQ.

a. Utilice un cliente VNC para iniciar sesión en el servidor de sucesos y escriba los mandatos indicados a continuación para abrir el explorador deWebSphere MQ:

```
xhost +
su - mqm
strmqcfg &
```

Nota: Si se abre la página de bienvenida, ciérrela.

b. Expanda **IBM WebSphere MQ** > **Queue Managers** > **IOC.MC.QM** > **QueuesLocate** y seleccione la carpeta**Colas**.

c. En la tabla **Colas**, compruebe la **Profundidad de cola actual** de todas las colas que empiezan por **IOC**_. Por ejemplo, IOC_KPI_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY.

Una profundidad de cola superior a 0 durante cualquier periodo de tiempo puede indicar un problema.

5. Compruebe si los sucesos CAP llegan a la base de datos de IBM Intelligent Operations Center.

a. Utilice un cliente VNC para iniciar sesión en el servidor de datos y escriba los mandatos indicados a continuación para abrir el DB2 Control Center:

```
xhost +
su - db2inst1
Db2cc &
```

b. Haga clic en **IOCDB** > **tablas**, haga clic con el botón derecho en**Suceso** en el esquema **IOC_COMMON** y haga clic en **Abrir**. Verá una lista de los sucesos enviados al sistema.

c. Compruebe si los sucesos están en la base de datos.

Nota: Quizá necesite captar más filas, dependiendo de los sucesos de su sistema.

6. Para definir el rastreo en el servidor de portal, siga estos pasos:
   a. Inicie sesión en la consola de administración en `http://app-host:9060/ibm/console`, donde `app-host` es el nombre completo de host del servidor de aplicaciones.
   b. Pulse **Resolución de problemas** > **Registros y rastreo**.
   c. Pulse **WebSphere_Portal** > **Cambiar detalles de nivel de registro**.
   d. Haga clic en la pestaña **Tiempo de ejecución**, copie el siguiente mandato y haga clic en **Aceptar**.

```
*=warning: com.ibm.iss.*=all: com.ibm.ioc.*=all
```

   e. Para ver un registro, escriba el siguiente mandato:

```
cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal
tail –f trace.log
```

   Para obtener más información acerca de la visualización de registros, consulte el enlace situado al final del tema.

Conceptos relacionados:

"Habilitación de seguimientos y visualización de archivos de registros" en la página 301
Para solucionar un problema en IBM Intelligent Operations Center , es posible que tenga que analizar los archivos de registro en varios sistemas. Los siguientes temas le proporcionan orientación sobre cómo acceder a los archivos de registro.

Mecanismo de autenticación no disponible

Si recibe el mensaje de error `HPDIA0119W El mecanismo de autenticación no está disponible` después de iniciar sesión en WebSphere Portal, revise el estado del servidor Tivoli Directory Server y el Proxy Tivoli Directory Server para el servidor de aplicación.

Procedimiento

1. Inicie sesión en el servidor de gestión como `ibmadmin` y especifique los mandatos siguientes:

```
su – ibmadmin
cd /opt/IBM/ISP/mgmt/scripts
./iopmgmt.sh  status tds contraseña_topología
```

   Si el servidor se está ejecutando, se muestra un mensaje similar al ejemplo siguiente:

```
Ejecutando mandato de consulta.....completado.
 IBM Tivoli Directory Server [ on ]
El mandato se ha completado correctamente.
```

2. Si el servidor no se está ejecutando, escriba`./iopmgmt.sh start tds topology_password`
3. Si el servidor no se está ejecutando después de que complete los pasos 1 y 2, inicie sesión en el servidor de gestión como `ibmadmin` y especifique los mandatos siguientes:

```
su – ibmadmin
cd /opt/IBM/ISP/mgmt/scripts
./iopmgmt.sh  status tdspxyapp contraseña_topología
```

   Si el servidor se está ejecutando, se muestra un mensaje similar al ejemplo siguiente:

```
Ejecutando mandato de consulta.....completado.
IBM Tivoli Directory Server [ on ]
El mandato se ha completado correctamente.
```

4. Si el servidor no se está ejecutando, escriba `./iopmgmt.sh start tdspxyapp`*topology_password*

El servidor de terceros no responde

Si recibe el mensaje de error `El servidor de terceros no se está ejecutando` después de que inicia sesión en el portalWebSphere Portal, verifique el estado de WebSphere Portal.

Procedimiento

1. Inicie sesión en el servidor de administración como `ibmadmin` y escriba el mandato siguiente:

   ```
   su – ibmadmin
   cd /opt/IBM/ISP/mgmt/scripts
   ./iopmgmt.sh  status wpe contraseña_topología
   ```

   Si el portal se está ejecutando, se muestra un mensaje similar al siguiente:

   ```
   Ejecutando mandato de consulta.....completado.
   IBM WebSphere Portal Extend [ on ]
   El mandato se ha completado correctamente.
   ```

2. Si el portal no se está ejecutando, especifique `./iopmgmt.sh start wpe` *`contraseña_topología`*.

No se muestran actividades en el portlet Mis actividades

Si no ve ninguna actividad en el portlet Mis actividades, puede deberse a varias causas que se describen en las secciones siguientes.

Resolución de problemas con los datos de ejemplo

Utilice los datos de ejemplo para crear un suceso y utilizar los resultados para definir la posible causa por la que no se muestren las actividades.

Procedimiento

1. Inicie sesión en la interfaz de administración de IBM Intelligent Operations Center como `wpsadmin`.
2. Crea un suceso “Huracán cercano”:
   a. En el portlet Mapa, haga clic con el botón derecho en el mapa y pulse **Añadir suceso**.
   b. En **Tipo de suceso**, seleccione **Huracán cercano**. El resto de campos se completarán automáticamente.
   c. En **Urgencia**, seleccione **Prevista**.
   d. Conserve los valores predeterminados en el resto de parámetros y haga clic en **Aceptar**.

   Los parámetros del suceso "Huracán cercano" se correlacionarán con una muestra de procedimiento operativo estándar en matriz de selección del procedimiento de operación estándar.
3. Tras aproximadamente 5 minutos, verifique si la nueva actividad que corresponde al suceso "Huracán cercano" se muestra en el portletMis actividades.

Resultados

- Si la actividad correspondiente al suceso "Huracán cercano" no se muestra en el portlet Mis actividades, el problema de que las actividades no se muestren para otro usuario podría deberse a un problema conTivoli Service Request Manager.
- Si la actividad correspondiente al suceso "Huracán cercano" se muestra en el portlet Mis actividades, el problema de que las actividades no se muestren para otro usuario podría deberse a una de las razones siguientes:
  – Los permisos del usuario no se han configurado correctamente.
  – No se ha configurado correctamente un procedimiento operativo estándar.
  – El matriz de selección del procedimiento de operación estándar no se ha configurado correctamente.

Referencia relacionada:

"procedimientos de operación estándar, flujos de trabajo de muestra y recursos" en la página 142
El procedimientos de operación estándar, flujos de trabajo de muestra y los recursos se proporcionan cuando instala IBM Intelligent Operations Center versión 1.5.

Verificación del estado de Tivoli Service Request Manager

Si no se muestra ninguna actividad en el portlet Mis actividades al crear un suceso con datos de ejemplo, utilice el siguiente procedimiento para resolver los problemas deTivoli Service Request Manager.

Antes de empezar

Asegúrese de que la contraseña de administración de Tivoli Service Request Manager se ha cifrado correctamente. Para obtener más información, consulte el enlace que encontrará al final del procedimiento.

Acerca de esta tarea

Elija una de las opciones siguientes.

Procedimiento

- Utilice Herramienta de control de plataforma para comprobar el estado de Tivoli Service Request Manager:
  1. Inicie sesión en servidor de sucesos como `ibmadmin` con el mandato`putty`.
  2. Vaya al directorio `opt/IBM/ISP/mgmt/scripts`.
  3. Utilice Herramienta de control de plataforma para obtener el estado de Tivoli Service Request Manager y detener e iniciar Tivoli Service Request Manager. Para obtener más información sobre la ejecución de Herramienta de control de plataforma, consulte el enlace al final del procedimiento.
- De forma alternativa, para reiniciar manualmente Tivoli Service Request Manager, si los pasos indicados a continuación:
  1. Inicie sesión en servidor de sucesos como `ibmadmin` con el mandato`putty`.
  2. Para detener Tivoli Service Request Manager, escriba los mandatos siguientes:

     ```
     cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin
     ./stopServer.sh MXServer1 -user waswebadmin -password password
     ./stopNode.sh -user waswebadmin -password password
     ../../ctgDmgr01/bin/stopManager.sh -user waswebadmin -password password
     ```

     donde *password* es la contraseña de topología.
  3. Para iniciar Tivoli Service Request Manager, escriba los mandatos siguientes:

     ```
     cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin
     ../../ctgDmgr01/bin/startManager.sh
     ./startNode.sh -user waswebadmin
     ./startServer.sh MXServer1
     exit
     ```

Tareas relacionadas:

"Consulta del estado de los servicios" en la página 206
Herramienta de control de plataforma está disponible para determinar el estado de los servicios de IBM Intelligent Operations Center.

"Inicio de los servicios" en la página 199
Herramienta de control de plataforma está disponible para iniciar los servicios en ejecución en los servidores IBM Intelligent Operations Center.

"Detención de los servicios" en la página 203
Herramienta de control de plataforma está disponible para detener los servicios de IBM Intelligent Operations Center.

"Cifrado de la contraseña administrativa de Tivoli Service Request Manager" en la página 61
Utilice el siguiente procedimiento para cifrar la contraseña administrativa deTivoli Service Request Manager en Tivoli Netcool/Impact.

Verificación de permisos de usuario

Compruebe si un usuario tiene permiso para ver las actividades asociadas con procedimiento operativo estándar.

Procedimiento

1. Para abrir el portlet Procedimientos operativos estándar, en la interfaz de administración de WebSphere Portal, pulse **Intelligent Operations** > **Herramientas de personalización** > **Procedimientos operativos estándar**.
2. Para abrir la aplicación Matriz de selección de procedimiento operativo estándar, pulse **Matriz de selección de procedimiento operativo estándar**.
3. En la columna **SoP Name**, ubique el nombre de un procedimiento operativo estándar para el que desee verificar los permisos de un usuario.
4. Junto al campo **Nombre SoP**, haga clic en el icono **Menú Detalles** y a continuación en **Ir a procedimiento operativo estándar**.
5. Junto al campo **Grupo de propietarios**, haga clic en el icono **Menú Detalles** y a continuación en **Ir a grupos de personas**.
6. Compruebe si el usuario es miembro del grupo de personas.

Qué hacer a continuación

Si el usuario no es miembro del grupo de personas, lleve a cabo una de las acciones siguientes:

- No dé al usuario permiso para ver las actividades asociadas con el procedimiento operativo estándar.
- Añada el usuario al grupo de personas para que pueda ver todas las actividades asignadas algrupo de personas.
- Añada el usuario a otro grupo de personas asociado conprocedimiento operativo estándar.

Para obtener más información sobre la configuración de usuarios, consulte el enlace situado al final de esta tarea.

Tareas relacionadas:

"Configuración de nuevos usuarios en Tivoli Service Request Manager" en la página 130
Cuando añade un usuario a IBM Intelligent Operations Center, asigna permisos y grupos de personas para el usuario en Tivoli Service Request Manager.

Verificación de la asociación de un flujo de trabajo con un procedimiento operativo estándar

Cree un suceso cuyos parámetros coincidan con un conjunto de criterios de selección definido en elmatriz de selección del procedimiento de operación estándar. Compruebe si las actividades de flujo de trabajo asociadas se muestran en el portletMis actividades.

Acerca de esta tarea

Para obtener más información sobre cada uno de los pasos, consulte los enlaces situados al final del procedimiento.

Procedimiento

1. Cree un flujo de trabajo.
2. Cree un procedimiento operativo estándar y asócielo con el flujo de trabajo creado en el paso anterior.
3. Cree una entrada para el procedimiento operativo estándar en el matriz de selección del procedimiento de operación estándar.
4. En el portlet Mapa , cree un suceso cuyos parámetros coincidan con los definidos en el matriz de selección del procedimiento de operación estándar.
5. Compruebe si las actividades de flujo de trabajo asociadas se muestran en el portletMis actividades.

Qué hacer a continuación

Si no se muestra ninguna actividad en el portlet Mis actividades, compruebe si ha configurado el flujo de trabajo, procedimiento operativo estándar, matriz de selección del procedimiento de operación estándar y el suceso correctamente. Si la configuración es correcta, compruebe el archivo de registro de políticas de Tivoli Netcool/OMNIbus y los archivos de registro de Tivoli Service Request Manager.

Conceptos relacionados:

"Mapa" en la página 285
Uso del portlet Mapa para ver sucesos y recursos en un mapa.

"Mis actividades" en la página 290
El portlet Mis actividades muestra una lista dinámica de actividades que son propiedad del grupo del que es miembro el usuario que tiene sesión iniciada en la interfaz.

Tareas relacionadas:

"Creación de flujos de trabajo" en la página 132
En Tivoli Service Request Manager, puede crear flujos de trabajo que puede incluir como tareas automáticas en las actividades de procedimiento operativo estándar .

"Creación de procedimientos de operación estándar" en la página 133
Cree un procedimiento operativo estándar, y asígnelo a un grupo propietario. Los usuarios se asignan a un grupo propietario a través de su pertenencia a un grupo de personas.

"Definición de parámetros en la matriz de selección del procedimiento de operación estándar" en la página 135
En la matriz de selección del procedimiento de operación estándar, defina los parámetros de suceso que determinan si un procedimiento operativo estándar se selecciona para un suceso determinado.

Comprobación de los archivos de registro

Compruebe el archivo de registro de políticas de Tivoli Netcool/OMNIbus y el archivo de registro deTivoli Service Request Manager.

Procedimiento

- Compruebe el archivo de registro de políticas de Tivoli Netcool/OMNIbus:
  1. Habilite el archivo de registro de políticas de Tivoli Netcool/OMNIbus. Para obtener más información sobre la habilitación y uso del archivo de registro, consulte el enlace que encontrará al final del procedimiento.
  2. En el archivo de registro de políticas de Tivoli Netcool/OMNIbus, ubique un suceso y busque`CallMaximoEnterpriseServices`. El archivo de registro de políticas de Tivoli Netcool/OMNIbus analizará los sucesos por parámetro, por ejemplo, `Categoría` y `Gravedad` e indicará cada suceso con el ID de orden de trabajo asociada. Puede hacer que los sucesos coincidan con el matriz de selección del procedimiento de operación estándar. Si un suceso no aparece en el archivo de registro de políticas deTivoli Netcool/OMNIbus, quizá no haya procedimiento operativo estándar que coincidan con los parámetros del suceso.
  3. Busque `server error 500`, que indica si existen errores del servidor de Tivoli Service Request Manager. Si ve este error, compruebe el archivo de registro de Tivoli Service Request Manager. Siga el enlace situado al final de este procedimiento.
- Compruebe el archivo de registro de Tivoli Service Request Manager. Para obtener más información sobre la habilitación y uso del archivo de registro, consulte el enlace que encontrará al final del procedimiento.

Tareas relacionadas:

"Habilitación y visualización de archivos de registro de Tivoli Netcool/Impact" en la página 305

"Habilitación de rastreo y visualización de archivos de registro para Tivoli Service Request Manager" en la página 302

Los datos de KPI no se muestran en los portlets Estado o Obtención de detalles de indicador clave de rendimiento

Si los datos de KPI no se muestran en los portlets Estado o Obtención de detalles de indicador clave de rendimiento, siga los pasos de este procedimiento hasta que el problema se haya resuelto.

Procedimiento

1. Para comprobar el estado de IBM WebSphere Business Monitor, inicie sesión en la consola de administración de WebSphere Application Server. Para obtener información sobre el acceso a las consolas de administración, vaya al enlace que hay al final del tema.
2. Si IBM WebSphere Business Monitor se ha detenido, reinícielo. Si IBM WebSphere Business Monitor no se ha detenido, primer deténgalo y después reinícielo. Si el problema sigue si resolverse, vaya al paso 3.
3. Compruebe los registros de IBM WebSphere Business Monitor para investigar y resolver problemas conIBM WebSphere Business Monitor. Para obtener información sobre la comprobación de registros, vaya al enlace que hay al final del tema.
4. Cuando haya resuelto todos los problemas de IBM WebSphere Business Monitor, inicie sesión en la consola de administración de WebSphere Application Server para reiniciar IBM WebSphere Business Monitor.

Conceptos relacionados:

"Archivos de registro de Servidor de aplicaciones" en la página 301
Utilice los procedimientos siguientes para habilitar rastreos y ver los registros para algunos de los sistemas de servidor de aplicaciones.

"Consolas de administración" en la página 207
Utilice el portlet Consolas de administración para administrar los servicios proporcionados por la solución.

Los sucesos no se actualizan en los portlets Estado o Obtención de detalles de indicador clave de rendimiento

Si los datos de sucesos de KPI no se actualizan en los portlets Estado o Obtención de detalles de indicador clave de rendimiento, siga los pasos de este procedimiento hasta que el problema se haya resuelto.

Procedimiento

1. Para confirmar si las actualizaciones de sucesos de KPI llegan a IBM Intelligent Operations Center, siga el enlace *Los sucesos nuevos no se muestran en el portlet Detalles* que encontrará al final de este tema y complete los pasos indicados.
2. Confirme que los sucesos llegan a IBM WebSphere Business Monitor.
   a. Inicie sesión en la consola de administración de WebSphere Application Server.Para obtener información sobre el acceso a las consolas de administración, vaya al enlace que hay al final del tema.
   b. Haga clic en **Resolución de problemas** > **Modelos de supervisor** > **Secuencias de sucesos anómalos**. Suprima todos los sucesos de KPI que aparezcan en esta página.
   c. Reinicie IBM WebSphere Business Monitor.
   d. Haga clic en **Aplicaciones** > **Servicios de supervisor** > **Gestión de sucesos registrados** > **Habilitar/Inhabilitar registro de sucesos** y habilite el registro de sucesos.
   e. Haga clic en **Aplicaciones** > **Servicios de Monitor** > **Gestión de sucesos registrados** > **Gestión de sucesos**. Compruebe en esta página si hay al menos dos sucesos creados para cada KPI enviado al IBM Intelligent Operations Center.
3. Confirme que las actualizaciones de sucesos de KPI llegan al portlet Indicadores clave de rendimiento. Para obtener más información sobre el portlet Indicadores clave de rendimiento, vaya al enlace situado al final de este tema. Si los valores de los KPI se actualizan en el portlet Indicadores clave de rendimiento, estos también se actualizarán en IBM WebSphere Business Monitor.

Conceptos relacionados:

"Consolas de administración" en la página 207
Utilice el portlet Consolas de administración para administrar los servicios proporcionados por la solución.

"Indicadores clave de rendimiento" en la página 173
Utilice el portlet Indicadores clave de rendimiento para personalizar los indicadores clave de rendimiento (ICR) y su visualización jerárquica en IBM Intelligent Operations Center.

Tareas relacionadas:

"Los sucesos nuevos no se muestran actividades en el portlet Detalles" en la página 340
Si los sucesos nuevos no se muestran actividades en el portlet Detalles, siga los pasos indicados a continuación para resolver el problema.

Capítulo 10. Referencia

Estos temas contienen información de referencia adicional que le resultará de ayuda.

Productos y componentes incluidos con IBM Intelligent Operations Center

La solución de IBM Intelligent Operations Center instala varios componentes y productos de software.

Los productos y componentes de software y los servidores en los que están instalados se muestran en Tabla 100.

Tabla 100. Productos instalado con IBM Intelligent Operations Center

Producto	Servidor de aplicaciones	Servidor de datos	Servidor de sucesos	Servidor de gestión
IBM WebSphere Business Monitor 7.5	instalados	no instalado	no instalado	no instalado
IBM Cognos Business Intelligence 10.1.1	instalados	no instalado	no instalado	no instalado
DB2 Enterprise Server Edition con DB2 Spatial Extender 9.7.0.5	no instalado	instalados	no instalado	instalados
Servicios de modelo semántico	no instalado	no instalado	no instalado	instalados
IBM ILOG CPLEX Optimization Studio 12.4	instalados	no instalado	no instalado	no instalado
Jazz Foundation Server (para Servicios de modelo semántico) 3.0.1	no instalado	no instalado	no instalado	instalados
Lotus Domino 8.5.3.1	no instalado	no instalado	instalados	no instalado
Lotus Sametime Standard 8.5.2 + IFR1	no instalado	no instalado	instalados	no instalado
Tivoli Access Manager for e-Business 6.1.1.4	no instalado	no instalado	no instalado	instalados
Tivoli Composite Application Manager 7.1	no instalado	no instalado	no instalado	instalados
Tivoli Directory Integrator 7.1.0.5	no instalado	no instalado	no instalado	instalados
Tivoli Directory Server 6.3.0.8	no instalado	instalados	no instalado	no instalado
Tivoli Identity Manager 5.1	no instalado	no instalado	no instalado	instalados
Tivoli Monitoring 6.2.2.1	no instalado	no instalado	no instalado	instalados

Tabla 100. Productos instalado con IBM Intelligent Operations Center (continuación)

Producto	Servidor de aplicaciones	Servidor de datos	Servidor de sucesos	Servidor de gestión
Tivoli Netcool/Impact 5.1.1.1 + IF003	no instalado	no instalado	instalados	no instalado
Tivoli Netcool/OMNIbus 7.3.1.2 y analizador XML	no instalado	no instalado	instalados	no instalado
Tivoli Service Request Manager 7.2.1.2	no instalado	no instalado	instalados	no instalado
Paquete de características de WebSphere Application Server 1.1.0.0 para Web 2.0 y dispositivo móvil	instalados	no instalado	no instalado	no instalado
WebSphere Application Server Network Deployment 7.0.0.21	instalados	no instalado	no instalado	instalados
WebSphere Application Server 6.1.0.29 paraTivoli Service Request Manager	no instalado	no instalado	instalados	no instalado
WebSphere Message Broker 8.0	no instalado	no instalado	instalados	no instalado
WebSphere MQ 7.0.1.7	no instalado	no instalado	instalados	no instalado
WebSphere Operational Decision Management 7.5.1 (Motor de reglas)	instalados	no instalado	no instalado	no instalado
WebSphere Portal Enable 7.0.0.2	instalados	no instalado	no instalado	no instalado

Procesos que se ejecutan bajo la cuenta `raíz`

Una vez que se ejecuta Cyber Hygiene, aún se deben ejecutar algunos procesos bajo la cuenta `raíz`.

Los procesos que se ejecutan bajo la cuenta `raíz` pueden ser vulnerables en caso de que el usuario o proceso puedan obtener privilegios `raíz` a través de la elevación de privilegios. Normalmente esto solo resulta un problema en caso de solicitudes de procesamiento de servicios originadas por un usuario. Las solicitudes originadas por un usuario pueden contener entradas configuradas de forma maliciosa que pueden poner en peligro al servidor. Las solicitudes del usuario de procesamiento de servicios son sistemas que proporcionan interfaces del usuario o interfaces de programación de aplicaciones accesibles(API).

Los daemons de Linux normalmente no están en peligro, ya que suelen iniciarse, detenerse o responder a eventos en el sistema bien definidos. En muchos casos, estos daemons deben ejecutarse como cuenta `raíz`

para poder controlar otros procesos o responder a eventos críticos del sistema. Mientras un servidor accesible por el usuario no se ejecute como raíz en sí mismo, los daemons que se ejecutan bajo la cuenta raíz no suponen una exposición peligrosa.

Con la excepción deTivoli Netcool/OMNIbus, todos los servidores de productos deIBM Intelligent Operations Center están configurados con ID sin privilegios de sistema. Tivoli Netcool/OMNIbus proporciona servicios de supervisión y gestión en todos los hosts y servidores de IBM Intelligent Operations Center.

Tabla 101 indica los procesos que continúan en ejecución como cuenta raíz una vez ejecutado Cyber Hygiene.

Tabla 101. El entorno de IBM Intelligent Operations Center procesa la ejecución como raíz

Servidor	Producto	Nombre de proceso	Explicación
servidor de datos y servidor de gestión	DB2	db2wdog	Este proceso de daemon recibe eventos del sistema y los propaga a diversos procesos hijo. El proceso db2wdog gestiona los procesos db2sync y requiere una gestión de nivel raíz.
servidor de datos y servidor de gestión	DB2	db2chkpwd	Este daemon autentica el ID de usuario y la contraseña del usuario o aplicación que se conecta a la base de datos. El proceso db2chkpwd necesita leer el archivo de contraseñas /etc/shadow.
servidor de datos y servidor de gestión	DB2	/opt/IBM/DB2/bin/db2fmcd	Este daemon sirve de coordinador de supervisión de anomalías. Se debe ejecutar como raíz para supervisar todas las instancias DB2.
servidor de datos y servidor de gestión	DB2	/usr/sbin/rcst/bin/rmcd y /usr/sbin/rcst/bin/IBM.ConfigRMd	Estos mandatos gestionan la solución de alta disponibilidad de DB2. Necesitan acceso a todas las base de datos de los servidores configurados para la alta disponibilidad.
servidor de sucesos	Agentes IBM Tivoli Monitoring para Lotus Domino	kgbagent, kgbclient, kslagent	Estos agentes de supervisión deben ejecutarse como raíz para realizar el seguimiento de la actividad del servidor de Lotus Domino.
servidor de aplicaciones, servidor de sucesos y servidor de gestión	IBM HTTP Server	httpd -d, http -f	Linux requiere acceso raíz para escuchar en los puertos inferiores al 1024. Los puertos HTTP estándar son los puertos 80 a 443. IBM Intelligent Operations Center utiliza el puerto 82. Los procesos httpd -d yhttp -f se deben ejecutar como raíz. Cualquier configuración alternativa es responsabilidad de la instalación como parte de la política de seguridad y red global y la configuración.
servidor de datos	Agentes de IBM Tivoli Monitoring	klzagent, kcawd	Se trata de procesos de agentes de gestión y supervisión. Estos procesos supervisan los procesos y recursos del sistema operativo y aplicaciones.
servidor de aplicaciones	Agentes de IBM Tivoli Monitoring	klzagent, kcawd, khtagent, kynagent	Se trata de procesos de agentes de gestión y supervisión. Estos procesos supervisan los procesos y recursos del sistema operativo y aplicaciones.
servidor de sucesos	Agentes de IBM Tivoli Monitoring	klzagent, kcawd, khtagent, kynagent, kmcrca, kgbagent, kgbstart.sh, kgbclient, kslagent, kmqagent, /opt/IBM/ITM/JRE/lx8266/bin/java	Se trata de procesos de agentes de gestión y supervisión. Estos procesos supervisan los procesos y recursos del sistema operativo y aplicaciones.
servidor de gestión	Agentes de IBM Tivoli Monitoring	cms, kdsmain, KfwServices, klzagent, kcawd, kynagent, /opt/IBM/ITM/li6263/iw/java/jre/bin/java, /opt/IBM/ITM/li6263/iw/java/bin/java	Se trata de procesos de agentes de gestión y supervisión. Estos procesos supervisan los procesos y recursos del sistema operativo y aplicaciones.
servidor de sucesos	Tivoli Netcool/OMNIbus	/usr/ibm/common/acsi/jre/bin/java, /opt/IBM/netcool/omnibus/platform/linux2x26/bin/nco_pad	El proceso nco_pad es el daemon del agente de procesos que supervisa todos los agentes de procesos. El daemon requiere acceso a los recursos del sistema. El daemon del agente de procesos no presenta una interfaz de usuario. Solo gestiona otros procesos.

Excepciones de Cyber Hygiene

Una vez que se ejecuta Cyber Hygiene, aquí permanecen las excepciones conocidas a la configuración de seguridad preferida.

En una configuración ideal no deberían existir excepciones a los valores de prácticas más adecuada. No obstante, en la mayoría de los sistemas hay excepciones. Estas excepciones no representan un riesgo significativo, pero si no se comprenden pueden ser problemáticas. Por ejemplo, algunos programas pueden no ejecutarse con el conjunto de bits **suid**.

Los administradores de seguridad deben comprender las excepciones para poder verificar si su sistema se ve comprometido. Al realizar una exploración, los administradores del sistema podrían confundir las excepciones previstas con programas maliciosos.

Tabla 102. Excepciones de Cyber Hygiene a la configuración de seguridad preferida

Vulnerabilidad	Servidor	Instancia	Explicación
GEN000360: GID definido con valor en el rango de sistema para Linux (0-499).	servidor de datos	dasadm1	EL ID de grupo (GID) dasadm1 está definido en 102. Se trata del grupo de administración para los ID de instancias de tiempo de ejecución de DB2. Este grupo se crea automáticamente cuando se instala DB2.

Permisos de archivos que requieren la evaluación del administrador del sistema

Cyber Hygiene no realiza cambios para las exposiciones de todos los permisos de archivos y participaciones. Algunas deben ser evaluadas y corregidas por los administradores del sistema, ya que los cambios automáticos podrían provocar el mal funcionamiento de algunas funciones del sistema.

Cyber Hygiene realiza scripts de información de registro sobre recursos afectados potencialmente. Los administradores del sistema pueden revisar estos hallazgos y realizar los cambios apropiados en el sistema.

Los archivos de hallazgos se encuentran en el directorio/var/BA15/CH/results de cada servidor de IBM Intelligent Operations Center. El nombre del archivo es scanrem-combined-log-*fecha-hora*.log. La indicación de fecha y hora indica cuándo se ha ejecutado Cyber Hygiene.

Tabla 103 indica las vulnerabilidades y acciones recomendadas que requieren revisión.

Tabla 103. Vulnerabilidades que requieren la evaluación del administrador del sistema

STIGID	Descripción	Gravedad	Recomendación
GEN001220	Los archivos, aplicaciones y directorios de los directorios del sistema deben ser propiedad de una cuenta del sistema o cuenta de aplicaciones.	II	Revise la propiedad del recurso y cambie o realice la documentación manual necesaria.
GEN001240	Los archivos, aplicaciones y directorios de los directorios del sistema deben ser propiedad de un grupo del sistema o grupo de aplicaciones.	II	Revise la propiedad del grupo del recurso y cambie o realice la documentación manual necesaria.
GEN001500	El directorio de inicio, indicado para cada usuario en el archivo /etc/password, debe ser propiedad de un usuario.	II	Revise la propiedad del directorio de inicio y cambie manualmente la misma, o documente por qué no se puede modificar.

Tabla 103. Vulnerabilidades que requieren la evaluación del administrador del sistema (continuación)

STIGID	Descripción	Gravedad	Recomendación
GEN001520	El directorio de inicio, indicado para cada usuario en el archivo `/etc/password`, debe ser propiedad del grupo primario del usuario.	II	Revise la propiedad del grupo del directorio de inicio y cambie manualmente la misma, o documente por qué no se puede modificar.
GEN001560	Los archivos del directorio de inicio, distintos a los archivos de inicio, deben tener permisos nunca superiores a 750.	III	Si las excepciones aún no están documentadas, cambie los permisos.
GEN002520	Los directorios públicos deben ser propiedad de la cuenta `root` o de un ID del usuario de la aplicación.	II	Revise la propiedad y asígnela como sea necesario.
GEN002540	Los directorios públicos deben ser propiedad de `root`, `sys`, `bin` o de un grupo de aplicaciones.	II	Revise la propiedad y asígnela como sea necesario.

Certificaciones de seguridad de productos y componentes

Algunos de los productos y componentes incluidos como parte de la solución IBM Intelligent Operations Center disponen de certificaciones de seguridad.

Tabla 104. Certificaciones de seguridad de productos instalados con IBM Intelligent Operations Center

	Criterio común		FIPS 140-2		
Producto	**Release**	**Nivel**	**Release**	**¿Certificado?**	**IPV6**
IBM WebSphere Business Monitor	Ninguno	Ninguno	7.5	Sí	Sí
IBM Cognos Business Intelligence	10.1.1	Ninguno	Ninguno	Ninguno	Sí
DB2 Enterprise Server Edition con DB2 Spatial Extender	9.7	EAL4+ALC_FLR.1	9.1 FP2	Sí	Sí
IBM HTTP Server	7.0.0.19		7.0	Sí	Sí
Lotus Domino	Ninguno	Ninguno	8.0.1	Sí	Sí
Lotus Sametime Standard	Ninguno	Ninguno	8.5	Sí	Sí
Tivoli Access Manager for e-Business	6.0 FP3	EAL3+ALC_FLR.1	6.0	Sí	Sí
Tivoli Composite Application Manager	Ninguno	Ninguno	Ninguno	Ninguno	Sí
Tivoli Directory Integrator	Ninguno	Ninguno	7.0	Sí	Sí
Tivoli Directory Server	6.2	EAL4+ALC_FLR.1	6.1	Sí	Sí
Tivoli Identity Manager	5.0	EAL3+ALC_FLR.1	Ninguno	Ninguno	Sí
Tivoli Monitoring	Ninguno	Ninguno	6.2.0.1	Sí	Sí
Tivoli Netcool/Impact	Ninguno	Ninguno	5.1	Sí	Sí
Tivoli Netcool/OMNIbus y analizador XML	7.1	EAL2	Todos	Sí	Sí
Tivoli Service Request Manager	Ninguno	Ninguno	Todos	Sí	Sí
WebSphere Application Server Network Deployment	6.1.0.2	EAL4+ALC_FLR.1	Todos	Sí	Sí
WebSphere Application Server paraTivoli Service Request Manager	6.1.0.2	EAL4+ALC_FLR.1	Todos	Sí	Sí
WebSphere Message Broker	6.0.0.3	EAL4+ALC_FLR.2 (de)	6.1	Sí	Sí
WebSphere MQ	6.0.1.1.	EAL4+ALC_FLR.2	Todos	Sí	Sí
WebSphere Operational Decision Management (Motor de reglas)	Ninguno	Ninguno	Ninguno	Ninguno	Sí
WebSphere Portal Enable	5.0	EAL2	Todos	Sí	Sí

Los productos con certificación FIP 104-2 normalmente se deben al uso de los módulos IBM Crypto for C y Java. Los números de certificado de estos productos se muestran enTabla 105.

Tabla 105. Certificados FIPS 140-2

Módulo	Número de certificado
IBM Crypto for C (V8.0.0)	1433
IBM CryptoLite for Java (V4.2)	910
IBM CryptoLite for C (V4.5)	899
IBM Java JCE 140-2 Cryptographic Module	497
IBM Java JSSE FIPS 140-2 Cryptographic Module	409
IBM SSL Lite for Java	406

Información relacionada:

Criterios comunes: http://www.commoncriteriaportal.org/

Evaluaciones de seguridad para productos IBM

Biblioteca de archivos PDF

Este tema proporciona enlaces al contenido del Information Center en formato PDF.

El contenido del Information Center está disponible en el siguiente PDF para que pueda imprimirlo:

- IBM Intelligent Operations Center Information Center

Glosario

Este glosario incluye términos y definiciones para IBM Intelligent Operations Center.

Este glosario utiliza las siguientes referencias cruzadas:

- Véase le remite desde un término a un sinónimo preferido o desde un acrónimo o una abreviatura a la forma completa definida.
- Véase también le remite a un término relacionado u opuesto.

Para ver glosarios de otros productos de IBM, vaya a www.ibm.com/software/globalization/terminology (se abre en una nueva ventana).

A

Abstract Syntax Notation One (ASN.1)
El estándar internacional para la definición de la sintaxis de los datos de la información. Define un número de tipos de datos simples y especifica una notación para hacer referencia a estos tipos y para especificar los valores de estos tipos. Las notaciones ASN.1 se puede aplicar siempre que sea necesario para definir la sintaxis abstracta de la información sin restricción de ninguna manera sobre cómo se codifica la información para su transmisión.

ACL Véase lista de control de accesos.

activador
Mecanismo que detecta una incidencia y puede provocar un proceso adicional como respuesta.

administrador de usuarios
Persona que agrega los nuevos usuarios y garantiza la seguridad, dotando a los miembros usuarios de los grupos autorizaciones basadas en roles con los permisos adecuados.

alerta Un mensaje que señala un suceso o un cambio de estado del KPI (indicador clave de rendimiento).

almacenamiento dinámico
En la programación Java, un bloque de memoria que la máquina virtual Java (JVM) utiliza en tiempo de ejecución para almacenar objetos Java. La memoria de almacenamiento dinámico Java está gestionada por un colector de basura, que desasigna automáticamente los objetos Java que han dejado de utilizarse.

APAR Véase informe autorizado de análisis de programa.

APAR (informe autorizado de análisis de programa)
Solicitud de corrección de un defecto en un release soportado de un programa suministrado por IBM.

aplicación en nube
Aplicación que se amplía para que sea posible acceder a ella desde internet. Las aplicaciones en nube utilizan grandes centros de datos y potentes servidores que alojan servicios web y aplicaciones web.

archivador empresarial (EAR)
Tipo especializado de archivo JAR, definido por el estándar Java EE, utilizado para desplegar aplicaciones Java EE en servidores de aplicaciones Java EE. Un archivo EAR contiene componentes EJB, un descriptor de despliegue y archivos WAR (archivador web) para aplicaciones web individuales. Véase también archivo Java.

archivador Java (JAR)
Formato de archivo comprimido para almacenar todos los recursos necesarios para instalar y ejecutar un programa Java en un solo archivo. Véase también archivador empresarial.

archivo CSV
Un archivo de texto que contiene valores separados por comas. Habitualmente, se utiliza un archivo CSV para intercambiar archivos entre sistemas y aplicaciones de base de datos que utilizan distintos formatos:

archivo de forma
Formato de archivo digital para el software de sistemas de información geográfica.

asíncrono
Relativo a eventos que no están sincronizados en el tiempo o que no se producen a intervalos de tiempo regulares o predecibles.

ASN.1 Véase Abstract Syntax Notation One.

atributo
Característica o rasgo de una entidad que la describe; por ejemplo, el número de teléfono de un empleado es uno de sus atributos.

autenticación
Servicio de seguridad que suministra una prueba de que un usuario de un sistema informático es verdaderamente quien dice ser. Los mecanismos habituales para implementar este servicio son contraseñas y firmas digitales.

autorización
Proceso de otorgar a un usuario, sistema o proceso acceso completo o restringido a un objeto, recurso o función.

ayuda contextual
El texto explicativo que se puede ver, moviendo el cursor sobre el elemento de una interfaz gráfica de usuario (GUI), como un icono, un campo o cadena de texto. La ayuda contextual puede contener texto enriquecido y enlaces.

C

CAP Véase Protocolo común de alertas.

capa Una superposición que se puede colocar en el mapa para proporcionar información geoespacial adicional.

Capa de sockets seguros (SSL, del inglés Secure Sockets Layer)
Protocolo de seguridad que proporciona privacidad en las comunicaciones. Con SSL, las aplicaciones cliente/servidor se pueden ubicar de un modo diseñado para impedir las intrusiones, la manipulación y la falsificación de mensajes.

configuración
1. Manera en que está organizado e interconectado el hardware y software de un sistema, subsistema o red.
2. Proceso de describir para un sistema los dispositivos, características opcionales y productos de programa que se han instalado a fin de que puedan utilizarse dichas características. Véase también personalización.

Correlación de sucesos
El proceso de analizar datos de suceso para identificar patrones, causas comunes y causas raíz. La correlación de sucesos analiza los sucesos entrantes de estados predefinidos mediante reglas predefinidas y comparándolos con relaciones predefinidas.

D

desencadenador de alertas
Cambio de un valor de indicador clave de rendimiento (KPI) predefinido que causa una notificación de alerta que se enviará al portlet Coordinador - Alertas.

dominio
Una división individual de una operación de gran envergadura, que generalmente coincide con la estructura de la organización y la experiencia de las personas involucradas. Por ejemplo, una autoridad de la ciudad se divide en departamentos que se ocupan del transporte, el agua y la seguridad pública.

E

EAR Véase archivador empresarial (enterprise archive).

EJB Véase Enterprise JavaBeans.

Enterprise JavaBeans (EJB)
Arquitectura de componentes definida por Sun Microsystems para el desarrollo y el despliegue de aplicaciones de nivel empresarial, distribuidas y orientadas a objetos (Java EE).

esquema de XML
Mecanismo para describir y restringir el contenido de archivos XML indicando los elementos que están permitidos y en qué combinaciones. Los esquemas XML son una alternativa a las definiciones de tipo de documento (DTD) y se pueden utilizar para ampliar la funcionalidad en las áreas de definición de tipo, herencia y presentación de datos.

F

flujo de trabajo
Un conjunto específico de acciones adecuadas para un conjunto particular de circunstancias. La solución se puede personalizar para activar flujos de trabajo apropiados, por ejemplo, la conexión a los sistemas de respuesta de emergencia.

Formato de intercambio de directorios LDAP (LDIF)
Formato de archivo que se utiliza para describir información del directorio, así como cambios que hay que aplicar a un directorio, como que la información del directorio se puede intercambiar entre servidores de directorio que utilicen LDAP.

formulario de filtro
Formulario que sirve para seleccionar el contenido que se mostrará en el mapa y la lista.

G

GDDM
Véase Gestor de visualización de fecha gráfico.

geoespacial
Relativo a las características geográficas de la Tierra.

Gestor de visualización de fecha gráfico (GDDM)
Un sistema de gráficos de cálculo de IBM que define y muestra texto y gráficos para su salida en una pantalla o impresora.

GIS Véase sistema de información geográfica.

grupo Conjunto de usuarios que pueden compartir autorizaciones de acceso a recursos protegidos.

grupo de categorías de datos
Un grupo cuyos miembros tienen acceso a una categoría específica de datos, por ejemplo, datos médicos y de salud pública, o datos ambientales. La pertenencia a un grupo de categorías de datos se asigna para dar a un usuario el nivel apropiado de acceso a los datos. Cada usuario se añade como un miembro del grupo o grupos apropiados.

grupo de roles de usuario
Un grupo que asigna pertenencias para proporcionar a un usuario nuevo el nivel apropiado de acceso a la solución. Todos los usuarios nuevos se añaden como miembros de un grupo de roles apropiado. Hay diferentes niveles de permiso asociados con cada grupo de roles.

I

Identificador uniforme de recursos (URI)

1. Dirección exclusiva que se utiliza para identificar contenido en la web como una página de texto, un vídeo o un clip de sonido, una imagen estática o animada o un programa. El formato más común de URI es la dirección de página web, que es un formato particular o subconjunto de URI denominado localizador uniforme de recursos (URL). Un URI describe habitualmente cómo acceder al recurso, el sistema que contiene el recurso y el nombre del recurso (un nombre de archivo) en el sistema.
2. Serie de caracteres compacta para identificar un recurso físico o abstracto.

incidencia
Un suceso que no forma parte de la operación estándar de un servicio y causa o puede causar una interrupción o una reducción de la calidad de los servicios y la productividad del cliente. Consulte también suceso.

Indicador clave de rendimiento
Véase indicador clave de rendimiento.

indicador clave de rendimiento (KPI)
Medida cuantificable diseñada para realizar el seguimiento de uno de los factores de éxito críticos de un proceso de negocio.

inicio de sesión único (SSO)
Proceso de autenticación en el que el usuario puede acceder a más de un sistema o aplicación a través de un único ID de usuario y contraseña.

instancia de contexto de supervisión
La información de IBM WebSphere Business Monitor que se recopila en un punto específico en el tiempo dentro de un contexto de supervisión.

integración
La actividad de desarrollo de software en la que los componentes de software individuales se combinan en un todo ejecutable.

interceptor de asociación de confianza (TAI)
Mecanismo mediante el que se valida la confianza en el entorno del producto para cada solicitud que recibe el servidor proxy. El método de validación se acuerda entre el servidor proxy y el interceptor.

J

JAR Véase archivador Java.

Java EE
Ver Java Platform, Enterprise Edition.

Java Platform, Enterprise Edition (J2EE, Java EE)
Entorno para el desarrollo y el despliegue de aplicaciones empresariales, definido por Oracle. La plataforma Java EE consta de un conjunto de servicios, interfaces de programación de aplicaciones (API) y protocolos que proporcionan funcionalidad para el desarrollo de aplicaciones de varios niveles, basadas en la web. (Sun)

JavaScript Object Notation (JSON)
Un formato ligero de intercambio de datos que se basa en la notación literal de objetos de JavaScript. JSON es independiente del lenguaje de programación, sin embargo utiliza convenciones de lenguajes entre los que se incluyen C, C++, C#, Java, JavaScript, Perl, Python.

Java Virtual Machine (JVM)
Implementación de software de un procesador que ejecuta código Java compilado (applets y aplicaciones).

J2EE Véase Java Platform, Enterprise Edition.

JNDI Véase Java Naming and Directory Interface.

JNDI (Java Naming and Directory Interface)
Extensión de la plataforma Java que proporciona una interfaz estándar para los servicios de denominación y directorio heterogéneos.

JSON Véase JavaScript Object Notation.

JVM Siglas de Java Virtual Machine. Véase máquina virtual Java (JVM).

K

keyhole markup language (KML)
Una gramática XML y el formato de archivo para la creación de modelos y almacenamiento de las características geográficas como puntos, líneas, imágenes y polígonos.

KML Véase lenguaje de marcado de keyhole.

KPI anidado
Un KPI que se define como un hijo de un KPI padre.

KPI de agregación
Un valor de ICR (Indicador clave de rendimiento, o KPI, por sus siglas en inglés) que se calcula a partir de una métrica utilizando una función de agregación.

KPI de expresión
Un KPI que tiene su valor calculado a partir de los valores de los indicadores clave de rendimiento de otros.

L

latitud
La distancia angular de un lugar al norte o al sur del ecuador de la Tierra, por lo general se expresa en grados y minutos.

LDAP Véase Lightweight Directory Access Protocol.

LDIF Véase formato de intercambio de directorios LDAP.

Lenguaje de marcado ampliable (XML)
Metalenguaje estándar para definir lenguajes de marcación basado en SGML (Standard Generalized Markup Language).

lenguaje de ontología web (OWL)
Lenguaje que se utiliza para representar explícitamente el significado de términos de vocabularios y las relaciones entre estos términos. El OWL está destinado a ser utilizado cuando la información contenida en los documentos la van a procesar las aplicaciones, en oposición a situaciones en las que el contenido lo han de presentar únicamente a los seres humanos.

Lightweight Directory Access Protocol (LDAP)
Un protocolo abierto que utiliza TCP/IP para proporcionar acceso a directorios que admiten un modelo X.500 y que no necesita los recursos del protocolo de acceso a directorios (DAP) X.500 más complejo. Por ejemplo, LDAP puede utilizarse para ubicar personas, organizaciones y otros recursos en un directorio de Internet o intranet.

lista de control de acceso (ACL)
En seguridad de sistemas, una lista asociada a un objeto que identifica todos los asuntos que pueden acceder al objeto y sus derechos de acceso.

longitud
La distancia angular de un lugar al este o al oeste del meridiano Greenwich, England, generalmente expresado en grados y minutos.

LOS Véase nivel de servicio.

M

mapa base
Un mapa que muestra información de referencia de fondo, como geográfica, carreteras, puntos de referencia y límites de regiones, en el que se sitúa otra información temática. El mapa base se utiliza para referencia de ubicación y suele incluir una red de control geodésico como parte de su estructura.

mapa de ubicación
Un mapa o plan que contiene zonas interactivas que se han definido en IBM Intelligent Operations Center. Los sucesos se pueden asociar con una o varias de estas zonas. Por ejemplo, se puede definir un diagrama de zonas de asiento en un estadio deportivo, para que los sucesos que se produzcan se puedan asociar con el área correspondiente.

máscara
Elemento de una interfaz gráfica de usuario que se puede cambiar para alterar el aspecto de la interfaz sin afectar a su funcionalidad.

Matriz de selección de procedimiento operativo estándar
Matriz que contiene conjuntos únicos de parámetros de suceso que determinan si se inicia un procedimiento operativo estándar para un determinado suceso.

memoria caché
Memoria utilizada para mejorar los tiempos de acceso a instrucciones, datos o a ambas cosas. Los datos que residen en la memoria caché suelen ser una copia de los datos que residen en otro almacén más lento y menos caro, como un disco u otro nodo de red.

Modelo de ICR
Parte del modelo de supervisión que contiene los contextos KPI, que a su vez contienen indicadores clave de rendimiento y sus sucesos asociados.

modelo de supervisión
Modelo que describe los aspectos de gestión de rendimiento de negocio de un modelo de negocio, incluyendo eventos, métricas de negocio e indicadores clave de rendimiento (ICR) que son necesarios para supervisar la empresa en tiempo real.

modelo ISO
Conjunto de normas para la comunicación de datos, aprobado por la International Organization for Standardization (ISO). Los protocolos ISO permiten que sistemas suministrados por distintos proveedores puedan conectarse y comunicarse. Son la base de las normas de interconexión de sistemas abiertos (OSI).

N

nivel de servicio (LOS)
Una medida cualitativa utilizada en la industria del transporte por los ingenieros de tráfico para determinar la efectividad de los elementos de una infraestructura de transporte. Esta medida describe las condiciones operativas de tráfico tal como se definen en el Manual de Capacidad de Carreteras.

O

ontología
Especificación formal explícita de la representación de los objetos, conceptos y otras entidades que pueden existir en un área de interés y las relaciones entre ellos.

orden de trabajo (WO)
Registro que contiene información sobre el trabajo que debe llevarse a cabo.

OWL Véase lenguaje de ontología web.

P

página
En un entorno de portal, el elemento de interfaz que contiene uno o varios portlets.

panel de control
1. Una página web que puede contener uno o más asistentes que representan gráficamente los datos de negocio.
2. Una interfaz que integra datos procedentes de una variedad de fuentes y que proporciona una visualización unificada de información relevante y contextualizada.

paquete de recursos

1. Clase que contiene el texto para las páginas de tienda. Para crear y acceder a los paquetes de recursos se utiliza la API PropertyResourceBundle de Java.
2. Colección estructurada de datos que proporciona una correlación de clave-valor para datos (recursos) utilizados al localizar un programa. Los valores son comúnmente strings, pero pueden ser ellos mismos datos estructurados.

perfil de usuario
Descripción de un usuario que incluye información como por ejemplo, ID de usuario, nombre de usuario, contraseña, autoridad de acceso y otros atributos que se obtienen cuando el usuario inicia la sesión.

permiso de acceso a datos
El acceso a los datos de una categoría determinada, por ejemplo, datos médicos y de salud pública, o datos ambientales. Este acceso está asociado con un grupo de categorías de datos.

permiso de administrador
La autoridad otorgada a un administrador para que tengan acceso a crear, configurar y eliminar los recursos del portal o los usuarios. Esta autoridad es otorgada por la pertenencia a un grupo de roles de usuario.

permiso de autorización
Acceso a un portal, un recurso o los datos asociados con la pertenencia a un grupo.

permiso de usuario
La autorización otorgada a un usuario para que tengan acceso para ver y trabajar con los recursos del portal. Esta autoridad se otorga por la pertenencia a un grupo de roles de usuario.

personalización
1. Modificación de una página del portal o portlet por parte de un usuario. WebSphere Portal permite a un usuario personalizar una página de portal modificando el diseño de página y seleccionado qué portlets se visualizarán por dispositivo. Véase también personalización.
2. El proceso de describir los cambios opcionales a los valores predeterminados de un programa de software que ya está instalado y configurado en el sistema y se puede utilizar. Véase también configuración.

personalización
El proceso de habilitar información para dirigirla a los usuarios específicos basándose en las reglas de negocio y la información del perfil de usuario. Véase también personalización.

plug-in
Módulo de software que se puede instalar por separado que añade funcionalidad a un programa, aplicación o interfaz existente.

PMR Véase registro de gestión de problemas.

polígono
En la función GDDM, una secuencia de líneas rectas adyacentes que encierran un área.

política de KPI
Una política que determina si un evento de entrada es una actualización del suceso de KPI, a continuación, lo envía para procesar la generación de una actualización de KPI o una alerta en función de los parámetros.

portal Un solo punto de acceso seguro para diversa información, aplicaciones y personas que se puede personalizar.

portlet
Componente reutilizable que forma parte de una aplicación web que proporciona información o servicios específicos que se presentan en el contexto de un portal.

Procedimiento de operación estándar
Procedimiento que define una secuencia de actividades que se inician como respuesta a un suceso cuyos parámetros cumplen ciertas condiciones predefinidas.

Protocolo común de alertas (CAP)
Un formato sencillo pero general para el intercambio de alertas de emergencia de todos los peligros y avisos públicos sobre todo tipo de redes.

protocolo de control de transmisiones/protocolo Internet (TCP/IP)
Conjunto de protocolos de comunicación estándar de la industria y no propietario que proporciona conexiones fiables de extremo a extremo entre aplicaciones a través de redes interconectadas de distintos tipos.

R

RDF Véase Resource Description Framework (infraestructura de descripción de recursos).

RDF (Resource Description Framework)
Infraestructura que representa información en la web.

Really Simple Syndication (RSS)
Formato de archivo XML para contenido web corporativo basado en la especificación Really Simple Syndication (RSS 2.0). Los usuarios de Internet utilizan los formatos de archivo XML RSS para suscribirse a sitios web que proporcionan entradas RSS.

referencia lineal
Un marcador de referencia de ubicación a lo largo de una carretera, generalmente en un arcén, indicando su ubicación a lo largo de una ruta. Un ejemplo de un marcador es un mojón.

registro de gestión de problemas (PMR)
Número del mecanismo de soporte de IBM que representa una incidencia de servicio con un cliente.

Representational State Transfer (REST)
Estilo de arquitectura de software para sistemas de hipermedia distribuidos como, por ejemplo, World Wide Web. El término suele utilizarse para describir una interfaz simple que utiliza XML (o YAML, JSON, texto sin formato) a través de HTTP sin una capa de mensajería adicional como SOAP.

REST Véase Representational State Transfer.

RSS Consulte Really Simple Syndication.

S

servicio web
Aplicación modular autocontenida y autodescriptiva que puede publicarse, descubrirse e invocarse a través de una red mediante protocolos de red estándar. Normalmente, XML se utiliza para marcar datos, SOAP se utiliza para transferir datos, WSDL se utiliza para describir los servicios disponibles y UDDI se utiliza para listar qué servicios están disponibles. Vea también SOAP, Web Service Definition Language.

SGML
Véase Lenguaje de marcado generalizado estándar.

sistema de información geográfica (SIG)
Complejo de objetos, datos y aplicaciones que se utilizan para crear y analizar información espacial sobre características geográficas.

SOAP Protocolo ligero basado en XML para intercambiar información en un entorno distribuido descentralizado. SOAP se puede utilizar para consultar y devolver información e invocar servicios en Internet. Véase también servicio web.

solución
Una combinación de productos que se dirige a un problema de un cliente o proyecto en particular.

SPARQL
Un lenguaje de consulta para RDF que se utiliza para expresar consultas en orígenes de datos diferentes. La especificación W3 define la sintaxis y semántica del lenguaje de consulta SPARQL.

SSL Véase Secure Sockets Layer.

SSO Véase inicio de sesión único.

Standard Generalized Markup Language (SGML)
Un metalenguaje estándar para definir lenguajes de marcación basado en el estándar ISO 8879. SGML se centra en la estructuración de la información, en lugar de en la presentación; separa la estructura y el contenido de la presentación. También facilita el intercambio de documentos en un medio electrónico.

suceso Un hecho significativo que ocurre en un determinado lugar y tiempo. Véase también incidencia.

T

tabla de propiedades del sistema
Una tabla que almacena datos de configuración globales del sistema para IBM Intelligent Operations Center.

TAI Siglas de Trust Association Interceptor. Véase interceptor de asociación de confianza.

TCP/IP
Véase protocolo de control de transmisiones/protocolo Internet.

tema Elemento de estilo que proporciona un aspecto concreto a un lugar. El portal proporciona varios temas, similares a un fondo de pantalla virtual, que se pueden elegir al crear un lugar.

U

URI Véase identificador uniforme de recursos.

URL Véase localizador uniforme de recursos.

URL (localizador universal de recursos)
Dirección exclusiva de un recurso de información a la que se puede acceder en una red como Internet. El URL incluye el nombre abreviado del protocolo que se utiliza para acceder al recurso de información y la información que el protocolo utiliza para localizar el recurso de información.

usuario del portal autenticado
Un usuario que es miembro de un grupo paraguas dentro de WebSphere Portal autenticado con un perfil que contiene una contraseña y un ID de usuario.

V

vista de operaciones
Una página web que contiene portlets que pueden cooperar para facilitar el suministro de información coherente y la interacción a nivel de operaciones para supervisar los sucesos actuales y planificar sucesos futuros.

VNC Véase VNC, Virtual Network Computing.

VNC, Virtual Network Computing
Un sistema gráfico de compartición de escritorio que utiliza el protocolo Remote frame buffer (RFB) para controlar otro equipo de forma remota. Transmite los sucesos del teclado y el ratón de un equipo a otro, retransmitiendo las actualizaciones de pantalla gráfica en la otra dirección, a través de una red.

W

Web Map Service (WMS)
Un protocolo estándar para servir imágenes de mapas georeferenciadas a través de Internet generadas por un servidor de mapas con datos de una base de datos GIS. La especificación se desarrolló y publicó por primera vez el Consorcio Geoespacial Abierto en 1999.

Web Service Definition Language (WSDL)
Especificación basada en XML para describir los servicios de red como conjunto de puntos extremos que opera en mensajes que contienen información orientada a documentos o bien orientada a procedimientos. Véase también servicio web.

widget
Componente de interfaz de usuario reutilizable, como puede ser un botón, una barra de desplazamiento, un área de control o un área de edición de texto, que puede recibir datos de entrada procedentes del teclado o del ratón y comunicarse con una aplicación o con otro widget.Véase también widget común.

widget común
Widget proporcionado por IBM que no está asociado con un producto en particular. Véase también widget.

WMS Véase Web Map Service.

WO Véase orden de trabajo.

WSDL
Vea Web Service Definition Language.

X

XML Véase Extensible Markup Language (Lenguaje de códigos ampliable).

Z

zona lógica
Una agrupación lógica de activos o sucesos en un área geográfica.

Información adicional sobre el producto

Los siguientes recursos adicionales están disponibles en línea.

WebSphere Portal

- Página de soporte del producto WebSphere Portal : http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere_Portal
- Biblioteca de información WebSphere Portal : http://www.ibm.com/software/genservers/portal/library/
- Wiki de WebSphere Portal: http://www.lotus.com/ldd/portalwiki.nsf

WebSphere Application Server

- Página de soporte del producto WebSphere Application Server : http://www.ibm.com/software/webservers/appserv/was/support/
- Biblioteca de información WebSphere Application Server : http://www.ibm.com/software/webservers/appserv/was/library/index.html
- Information Center WebSphere Application Server 7.0.x : http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

Centros de información

- Cognos Centro de información de Business Intelligence: http://publib.boulder.ibm.com/infocenter/cbi/v10r1m1/index.jsp
- Information Center de DB2 : http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp
- Information Center de IBM ILOG CPLEX Optimization Studio : http://pic.dhe.ibm.com/infocenter/cosinfoc/v12r4/index.jsp
- Information Center de Lotus Domino : http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp
- Information Center de Lotus Notes : http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp
- Information Center de Lotus Sametime Standard : http://publib.boulder.ibm.com/infocenter/sametime/v8r5/index.jsp
- Information Center de Rational Application Developer : http://publib.boulder.ibm.com/infocenter/radhelp/v7r5/index.jsp?topic=/com.ibm.rad.legal.doc/helpindex_rad.html
- Information Center de Tivoli Access Manager : http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml
- Information Center de Tivoli Composite Application Manager : http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp
- Information Center de Tivoli Directory Integrator : http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDI.doc_7.1/welcome.htm
- Information Center de Tivoli Directory Server : http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml
- Information Center de Tivoli Identity Manager : http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml
- Information Center de Tivoli Netcool/Impact : http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcoolimpact.doc5.1.1/welcome.html
- Information Center de Tivoli Netcool/OMNIbus : http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcool_OMNIbus.doc_7.3.1/omnibus/wip/welcome.htm
- Information Center de Tivoli Service Request Manager : http://publib.boulder.ibm.com/infocenter/tivihelp/v32r1/index.jsp?topic=/com.ibm.srm.doc/srm_welcome.htm
- Information Center de IBM WebSphere Business Monitor : http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r0mx/index.jsp?topic=/com.ibm.btools.help.monitor.doc/home/home.html
- Information Center de WebSphere Message Broker : http://publib.boulder.ibm.com/infocenter/wmbhelp/v8r0m0/index.jsp
- Information Center de WebSphere MQ : http://publib.boulder.ibm.com/infocenter/wmqv7/v7r1/index.jsp
- Information Center de WebSphere Operational Decision Management : http://pic.dhe.ibm.com/infocenter/dmanager/v7r5/index.jsp

Redbooks

- Dominio Redbooks : http://www.redbooks.ibm.com/

Otros recursos web

- Formación y certificación Tivoli : http://www.ibm.com/software/tivoli/education/
- OASIS Protocolo Común de Alertas versión 1.2 http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html
- Sitio web de Red Hat: http://www.redhat.com/

Conceptos relacionados:

"Destinatarios" en la página 1
Este Information Center va dirigido a las personas que utilizan, instalan, administran y mantienen IBM Intelligent Operations Center. También contiene documentación de implementación para personalizar la solución e integrar los sistemas subyacentes externos que requiere IBM Intelligent Operations Center .

Aviso de copyright y marcas registradas

Aviso de copyright

Marcas registradas

Cognos, CPLEX, IBM, WebSphere, DB2, Domino, ILOG, Lotus, Notes, Rational, Tivoli, ibm.com, Passport Advantage, Sametime, Service Request Manager, Smarter Cities y Redbooks son marcas registradas deIBM Corporation en EE.UU., otros países, o ambos.

Microsoft, Internet Explorer, Windows, y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos, otros países, o ambos.

Pentium es una marca registrada de Intel Corporation o sus filiales en Estados Unidos y otros países

Linux es una marca registrada de Linus Torvalds en Estados Unidos y/o en otros países.

Adobe, Acrobat, Portable Document Format (PDF), y PostScript son marcas registradas de Adobe Systems Incorporated en los Estados Unidos y/o en otros países.

Oracle, Javascript y Java son marcas registradas de Oracle y/o sus filiales.

ArcGIS, EDN, StreetMap, @esri.com y www.esri.com son marcas comerciales, marcas registras o marcas de servicio de Esri en los Estados Unidos, la Comunidad Europea o algunas otras jurisdicciones.

Otros nombres pueden ser marcas registradas de sus respectivos propietarios.Otros nombres de empresas, productos y servicios pueden ser marcas registradas o de servicio de otros.

Avisos

Esta información se ha desarrollado para los productos y servicios que se comercializan en EE.UU.

Es posible que EIBM no ofrezca en otros países los productos, los servicios o las características que se describen en este documento. Póngase en contacto con el representante de IBM de su localidad para obtener información acerca de los productos y servicios que actualmente están disponibles en su zona. Las referencias a programas, productos o servicios de IBM no pretenden establecer ni implicar que sólo puedan utilizarse dichos productos, programas o servicios de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del cliente evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran el tema principal descrito en este documento. El suministro de este documento no le otorga ninguna licencia sobre estas patentes. Puede enviar consultas acerca de licencias, por escrito, a la dirección siguiente:

IBM Director of Licensing
IBM CorporationNorth Castle Drive
Armonk, NY 10504-1785
EE. UU.

Si tiene consultas sobre licencias relacionadas con información DBCS (de doble byte), póngase en contacto con el Departamento de propiedad intelectual de IBM en su país o envíelas, por escrito, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokio 103-8510, Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde tales disposiciones estén en contradicción con la legislación local:INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGUNA CLASE, EXPRESA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícitas ni explícitas, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no se aplique en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información de este documento está sujeta a cambios periódicos; dichos cambios se incorporarán en 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.

Todas las referencias hechas en este documento a sitios web que no son de IBM se proporcionan únicamente para su información y no representan en modo alguno una recomendación de dichos sitios web. El material de esos sitios web no forma parte del material de este producto de IBM y la utilización de esos sitios web se realizará bajo su total responsabilidad.

IBM puede utilizar o distribuir cualquier información que el usuario le proporcione de la manera que considere adecuada sin incurrir en ninguna obligación con el usuario.

Los licenciatarios de este programa que deseen obtener información acerca del mismo con el fin de: (i) intercambiar la información entre programas creados independientemente y otros programas (incluyendo éste) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
Department T81B F6/Building 503
4205 S. Miami Boulevard
Durham NC 27709-9990
EE. UU.

Dicha información puede estar disponible sujeta a los términos y condiciones adecuados, incluido, en algunos casos, el pago de una tasa.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material con licencia disponible para el mismo bajo los términos del Acuerdo de cliente de IBM, el Acuerdo de licencia de programa internacional de IBM o cualquier acuerdo equivalente entre las dos partes.

Cualquier dato de rendimiento aquí incluido se determinó en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Algunas mediciones pueden haberse hecho en sistemas que están a nivel de desarrollo y no existen garantías de que dichas mediciones sean las mismas en sistemas disponibles a nivel general. Además, algunas mediciones pueden haberse estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información referente a productos que no son de IBM se ha obtenido de los suministradores de estos productos, sus anuncios publicados u otras fuentes disponibles para el público. IBM no ha probado esos productos y no puede confirmar la exactitud del rendimiento, de la compatibilidad ni de ninguna otra declaración relacionada con productos que no sean de IBM. Las consultas acerca de las posibilidades de productos no IBM deben dirigirse a los suministradores de los mismos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales diarias. Para ilustrarlos de la mejor manera posible, estos ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos esos nombres son ficticios y cualquier parecido con nombres y direcciones utilizados por empresas reales es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje de origen que ilustran técnicas de programación en diferentes plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma, sin pagar nada a IBM, con los fines de desarrollar, utilizar, comercializar o distribuir programas de aplicación de acuerdo con la interfaz de programación de aplicaciones para la plataforma operativa para la cual se han escrito los programas de ejemplo. Estos ejemplos no se han probado completamente en todas las condiciones. Por lo tanto, IBM no puede garantizar ni dar por supuesta la fiabilidad, la capacidad de servicio ni el funcionamiento de estos programas. Los programas de ejemplo se ofrecen "TAL CUAL", sin garantía de ningún tipo. IBM no será responsable de los daños que surjan por el uso de los programas de ejemplo.

Marcas registradas

Cognos, CPLEX, IBM, WebSphere, DB2, Domino, ILOG, Lotus, Notes, Rational, Tivoli, ibm.com, Passport Advantage, Sametime, Service Request Manager, Smarter Cities y Redbooks son marcas registradas deIBM Corporation en EE.UU., otros países, o ambos.

Microsoft, Internet Explorer, Windows, y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos, otros países, o ambos.

Pentium es una marca registrada de Intel Corporation o sus filiales en Estados Unidos y otros países

Linux es una marca registrada de Linus Torvalds en Estados Unidos y/o en otros países.

Adobe, Acrobat, Portable Document Format (PDF), y PostScript son marcas registradas de Adobe Systems Incorporated en los Estados Unidos y/o en otros países.

Oracle, Javascript y Java son marcas registradas de Oracle y/o sus filiales.

ArcGIS, EDN, StreetMap, @esri.com y www.esri.com son marcas comerciales, marcas registras o marcas de servicio de Esri en los Estados Unidos, la Comunidad Europea o algunas otras jurisdicciones.

Otros nombres pueden ser marcas registradas de sus respectivos propietarios.Otros nombres de empresas, productos y servicios pueden ser marcas registradas o de servicio de otros.

Índice

Hoja de Comentarios

IBM Intelligent Operations Center
IBM Intelligent Operations Center
Documentación del producto
Versión 1 Release 5

Por favor, sírvase facilitarnos su opinión sobre esta publicación, tanto a nivel general (organización, contenido, utilidad, facilidad de lectura,...) como a nivel específico (errores u omisiones concretos). Tenga en cuenta que los comentarios que nos envíe deben estar relacionados exclusivamente con la información contenida en este manual y a la forma de presentación de ésta.

Para realizar consultas técnicas o solicitar información acerca de productos y precios, por favor diríjase a su sucursal de IBM, business partner de IBM o concesionario autorizado.

Para preguntas de tipo general, llame a "IBM Responde" (número de teléfono 901 300 000).

Al enviar comentarios a IBM, se garantiza a IBM el derecho no exclusivo de utilizar o distribuir dichos comentarios en la forma que considere apropiada sin incurrir por ello en ninguna obligación con el remitente.

Comentarios:

Gracias por su colaboración.

Para enviar sus comentarios:
- Envíelos por correo a la dirección indicada en el reverso.
- Envíelos por fax al número siguiente: 1-800-227-5088 (EE. UU. y Canadá)

Si desea obtener respuesta de IBM, rellene la información siguiente:

Nombre	Dirección
Compañía	
Número de teléfono	Dirección de e-mail

IBM
Information Development Department DLUA
P.O. Box 12195
Research Triangle Park, NC
USA

Impreso en España