IBM Security QRadar
Versión 7.2.6

Master Console v0.8.1

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 9.

Información sobre el producto

Este documento corresponde a IBM QRadar Security Intelligence Platform V7.2.6 y a todos los releases subsiguientes a menos sea reemplazado por una versión actualizada de este documento.

Contenido

Introducción a Master Console

Los administradores de IBM® Security QRadar utilizar Master Console para conocer el estado y obtener más información sobre los despliegues y los hosts.

Público al que se dirige

Esta guía está dirigida a todos los usuarios de QRadar responsables de investigar y gestionar la seguridad de la red. Para obtener esta información debe tener acceso a QRadar y conocer la red corporativa y las tecnologías de red.

Documentación técnica

Para buscar documentación del producto IBM Security QRadar en la web, incluida toda la documentación traducida, acceda al Knowledge Center de IBM (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Para obtener información sobre el acceso a más documentación técnica en la biblioteca de productos de QRadar, consulte Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0 &uid=swg21614644).

Cómo ponerse en contacto con el servicio de soporte al cliente

Para obtener información acerca de cómo ponerse en contacto con el servicio de soporte al cliente, consulte la nota técnica sobre soporte y descarga (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Declaración de buenas prácticas de seguridad

La seguridad de los sistemas de TI implica la protección de sistemas e información mediante la prevención, la detección y la respuesta a accesos indebidos desde dentro o fuera de la empresa. Un acceso indebido puede alterar, destruir o dar un uso inapropiado de la información o puede ocasionar daños o un uso erróneo de sus sistemas, incluidos los ataques a terceros. Ningún producto ni sistema de TI debe considerarse completamente seguro, y ningún producto, servicio o medida de seguridad por sí solo debe considerarse totalmente eficaz para evitar el acceso o el uso indebidos. Los sistemas, productos y servicios de IBM están diseñados como parte de un procedimiento global de seguridad de acuerdo con la legalidad vigente, lo que implica necesariamente procedimientos operativos adicionales, y pueden requerir otros sistemas, productos o servicios para ser más eficaces. IBM NO GARANTIZA QUE LOS SISTEMAS, PRODUCTOS O SERVICIOS SEAN INMUNES, O HAGAN QUE SU EMPRESA SEA INMUNE, A LAS CONDUCTAS MALICIOSAS O ILEGALES DE TERCEROS.

Tenga en cuenta lo siguiente:

El uso de este programa puede estar sujeto a diversas leyes o regulaciones, incluidas las relacionadas con la privacidad, la protección de datos, el empleo y las comunicaciones y el almacenamiento electrónicos. IBM Security QRadar solamente se puede utilizar con fines legales y de forma legal. El Cliente se compromete a utilizar este Programa de acuerdo con, y asume toda la responsabilidad en lo que se refiere al cumplimiento de las leyes, normativas y políticas aplicables. El

licenciatario declara que obtendrá o ha obtenido los consentimientos, permisos o licencias necesarios para permitir el uso legal de IBM Security QRadar.

Master Console

Novedades para administradores en Master Console en V0.8.1

Master Console V0.8.1 para IBM Security QRadar presenta la gestión de usuarios.

Gestión de usuarios

Master Console V0.8.1 presenta la gestión de usuarios que permite otorgar y controlar el acceso a Master Console para usuarios locales. Después de actualizar a Master Console V0.8.1 o una versión posterior, todos los usuarios de QRadar existentes se migran a Master Console como usuarios locales. Debe gestionar usuarios, incluyendo la adición de usuarios cambiando contraseñas en Master Console.  Más información....

Integración del proveedor de seguridad

Puede utilizar su infraestructura de seguridad de Active Directory o LDAP existente para configurar la autenticación de usuario.  Más información...

Instalación de Master Console

Instale o actualice Master Console instalando actualizaciones de software de Fix Central.

Procedimiento

1. Descargue el archivo de arreglos de software de Master Console de Fix Central (http://www-933.ibm.com/support/fixcentral).
2. Utilice un programa de software, como por ejemplo WinSCP, para copiar el arreglo de software de Master Console en el host de QRadar en el que instaló Master Console.
3. Utilice SSH para iniciar sesión en el QRadar donde ha copiado el arreglo de software de Master Console.
4. Detenga el servicio Tomcat tecleando el mandato siguiente:
   ```
   service tomcat stop
   ```
5. En la ventana de la consola del dispositivo de QRadar, instale Master Console tecleando el mandato siguiente:
   ```
   rpm -Uvh masterconsole-<versión#>.rpm
   ```
6. Reinicie el servicio Tomcat tecleando el mandato siguiente:
   ```
   service tomcat start
   ```

Resultados

Al ejecutar el archivo de instalación se actualiza la base de datos de Master Console y se reinician los servicios en el dispositivo QRadar.

Apertura de Master Console

Abra Master Console para supervisar el estado del despliegue de IBM Security QRadar subyacente y de los hosts gestionados.

Antes de empezar

- Debe instalar QRadar utilizando la clave de activación 8500 activation key (3L0C3S-2M0F3Q-6B1N0W-5N737F). Para obtener más información sobre cómo instalar QRadar, consulte la *Guía de instalación de IBM Security QRadar*.
- Debe ser administrador de QRadar para poder añadir, editar o eliminar consolas de QRadar.

Importante: Master Console no sustituye una consola de QRadar. Si está instalando Master Console en un entorno que ya tiene una consola de QRadar, mueva todos los procesadores de flujos y sucesos gestionados a otra consola antes de instalar Master Console. La instalación de Master Console sobrescribe todas las instalaciones anteriores en el dispositivo físico o virtual.

Procedimiento

1. Abra un navegador web y escriba el URL siguiente:
   `https://<Dirección_IP_de_consola_QRadar>`
2. Inicie la sesión en Master Console.

Visión general de la consola maestra

Utilice la consola maestra para supervisar uno o varios despliegues de IBM Security QRadar. Puede utilizar la consola maestra para ver las notificaciones del sistema, las velocidades de sucesos y las tasas de flujos, el uso de CPU por proceso, el uso de la memoria y más datos operativos.

Tarjetas de despliegue

La consola maestra representa los despliegues de QRadar en tarjetas de despliegue.

Las tarjetas de despliegue muestran la información siguiente para cada despliegue:

- Número de hosts gestionados y su estado. Por ejemplo, si el despliegue tiene 10 hosts gestionados y 5 tienen un estado crítico, la mitad del círculo alrededor del número 10 es de color rojo.
- Número de notificaciones del sistema críticas, de aviso e informativas de los últimos 15 minutos.
- Tasas de sucesos y flujos.

Las tarjetas de despliegue también contienen un menú donde puede editar los detalles del despliegue o suprimir el despliegue.

Pulse una tarjeta de despliegue para abrir la vista de hosts gestionados.

Visión general del hardware de Master Console

Master Console se diseñó para ejecutarse en el dispositivo QRadar 3105. Confirme que un dispositivo virtual o físico para Master Console cumple las especificaciones de la tabla siguiente.

- Utilice 8 procesadores para un máximo de 25.000 flujos por minuto (FPM) y de 1000 sucesos por segundo (EPS).
- Utilice 16 procesadores para un ,máximo de 200.000 FPM y de to 5000 EPS.

Para abrir Master Console, debe instalar QRadar, con un release 7.2.5 como mínimo y con la clave de activación 8500.

Tabla 1. Visión general de QRadar Log Manager 3105

Descripción	Valor
Interfaces	Dos interfaces de supervisión de red 10/100/1000 Base-T Una interfaz de gestión de QRadar 10/100/100 Base-T Una interfaz de módulo de gestión integrada 10/100 Base-T Dos puertos de 10 Gbps SFP +
Memoria	64 GB 8x8 GB 1600 MHz RDIMM
Almacenamiento	9 x 3,5 pulgadas 1 TB 7,2 K rpm NL SAS, 9 TB total, 6,2 TB utilizable (Raid 5)
Fuente de alimentación	Fuente de alimentación 750 W AC redundante dual
Dimensiones	29,5 pulgadas de fondo x 17,7 pulgadas de ancho x 2,4 pulgadas de alto
Componentes incluidos	Recopilador de sucesos Procesador de sucesos para procesar sucesos Almacenamiento interno para sucesos

Vista de hosts gestionados

En la vista de hosts gestionados se muestran todos los hosts del despliegue que ha seleccionado y las notificaciones del sistema correspondientes a cada host. La vista de hosts gestionados también está disponible en todos los despliegues de IBM Security QRadar V7.2.6 como **Estado del sistema** en la pestaña **Admin**.

Pulse una tarjeta Host gestionado para abrir la ventana Medidas de host, donde puede ver el uso de la CPU, las lecturas y escrituras de red, las lecturas y escrituras de disco, el uso de memoria, los sucesos por segundo (EPS) y los flujos por segundo (FPS).

La consola maestra muestra todos los hosts en la vista de hosts gestionados. Al pulsar la tarjeta de un host gestionado real, también puede ver las consultas en ejecución.

Pase el ratón sobre un gráfico para ver más información sobre el gráfico y la medida que se representa gráficamente.

Pulse **Ver despliegue** para abrir la página de inicio de sesión de la consola de QRadar para el despliegue en una pestaña nueva.

Supervisión de delitos en Master Console

Utilice Master Console para supervisar delitos de IBM Security QRadar de varios despliegues.

Procedimiento

1. Abra Master Console y pulse el icono Delitos  .
   Para obtener más información sobre la apertura de Master Console, consulte “Apertura de Master Console” en la página 1.

Los delitos de todos los despliegues se visualizan por orden de magnitud. La magnitud del delito está determinada por los valores de relevancia, gravedad y credibilidad. La magnitud tiene un valor numérico que determina el color de la tarjeta de delito. El orden de visualización es la magnitud, después el despliegue y después la hora de la última actualización.

Pulse el enlace de flecha en la tarjeta de delito para abrir el resumen de delito.

Tabla 2. Información de tarjeta de delito

Parámetro	**Descripción**
Nombre de despliegue	Un enlace a la consola de QRadar que generó el delito.
ID de delito	Un enlace al resumen de delito.
Dominio	El dominio del destino que generó el delito.
Origen de delito	La información depende del tipo de delito. Puerto de origen, se visualiza el puerto de origen del suceso que creó el delito.
Asignado a	Especifica el usuario asignado para investigar el delito. Si no se visualiza ningún usuario, puede asignar delitos a usuarios en QRadar. Para obtener más información sobre la asignación de delitos a QRadar, consulte la *Guía del usuario de IBM Security QRadar*.
Estado	ABIERTO, CERRADO u OCULTO. De forma predeterminada, el filtro solo visualiza los delitos abiertos.
Tipo de delito	Determinado por la regla que creó el delito. Por ejemplo, si el tipo de delito es de suceso de origen de registro, la regla que ha generado el delito correlaciona sucesos que están basados en el dispositivo que ha detectado el suceso.
Fecha de inicio	Especifica la fecha y hora del primer suceso o flujo que está asociado al delito.
Último suceso/flujo	Especifica el tiempo transcurrido desde que se observó el último suceso o flujo para el delito, categoría, dirección IP de origen o dirección IP de destino.
Red de origen	Especifica la red del dispositivo que ha intentado burlar la seguridad de un componente de la red.
Magnitud	Especifica la importancia relativa de la dirección IP de origen o destino.
Suceso/flujo	Especifica el número de sucesos o flujos que están asociados con la dirección IP de origen, dirección IP de destino, nombre de suceso, nombre de usuario, dirección MAC, origen de registro, nombre de host, puerto, origen de registro, dirección de ASN, dirección de IPv6, regla, ASN, aplicación, red o categoría.

Tabla 2. Información de tarjeta de delito (continuación)

Parámetro	Descripción
Recuento de orígenes	Especifica el número de direcciones IP de origen que están asociadas a delitos en la categoría. Si una dirección IP está asociada a delitos en cinco categorías de nivel bajo diferentes, la dirección IP de origen solo se cuenta una vez.
Recuento de destinos locales	Especifica el número de direcciones IP de destino local asociadas a la categoría.
Recuento de destinos remotos	Especifica el número de direcciones IP de destino remoto asociadas a la categoría.
Recuento de nombres de usuario	Especifica el número de nombres de usuario asociados a la categoría.

2. En la lista **Despliegue**, seleccione el despliegue para el que desea ver delitos.
3. Pulse el icono de renovación para actualizar los delitos listados.
4. Pulse el icono de filtro para ver los delitos visualizados por tipo de delito.

   El número de delitos generados por la combinación del despliegue seleccionado y el filtro aplicado se visualiza en la cabecera de página.

Adición de despliegues a la consola maestra

Un administrador de Master Console debe añadir a Master Console todos los despliegues de IBM Security QRadar que desea supervisar.

Antes de empezar

- Debe tener una señal de autorización. Para obtener más información, consulte el apartado "Creación de una señal de autorización para la consola maestra".
- Si organización necesita SSL seguro, asegúrese de que todos los despliegues que desea supervisar en Master Console tengan SSL seguro.

Procedimiento

1. Para añadir un despliegue, pulse el icono añadir (**+**).
2. Escriba un nombre para el despliegue.
3. Escriba la dirección IP o el nombre de host del despliegue.
4. Escriba la señal de autorización.
5. Pulse **Añadir despliegue**.
6. Si está añadiendo un despliegue con SSL no seguro y la organización no necesita SSL seguro, marque el recuadro de selección **Ignorar SSL no seguro** y pulse **Enviar**.

Creación de una señal de autorización para la consola maestra

Cree una señal de autorización para que Master Console pueda conectar con sus despliegues.

Procedimiento

1. En la pestaña **Admin**, pulse **Configuración del sistema**.
2. Pulse el icono **Servicios autorizados**.
3. Pulse **Añadir servicio autorizado**.

4. En la ventana **Gestionar servicios autorizados**, configure los parámetros.

Tabla 3. Parámetros de **Añadir servicio autorizado**

Parámetro	Descripción
Nombre del servicio	El nombre puede tener una longitud máxima de 255 caracteres.
Rol de usuario	Los roles de usuario asignados a un servicio autorizado determinan las funciones a las que dicho servicio puede acceder en la interfaz de usuario. Los administradores pueden crear un rol de usuario o asignar un rol de usuario predeterminado a la señal de autorización. Para la mayoría de las configuraciones, puede seleccionar **Todos**. **Nota:** El rol de usuario Admin proporciona más privilegios, lo que puede constituir un riesgo para la seguridad.

5. Pulse **Crear servicio**.
6. Anote el valor de la señal.

Adición de un usuario local

Después de la instalación de Master Console, los administradores añaden usuarios nuevos directamente en Master Console en lugar de en IBM Security QRadar.

Procedimiento

1. Pulse los valores ( ).
2. Pulse **Gestión de usuarios**.
3. Pulse el icono añadir **+** en la esquina superior derecha para abrir la ventana **Crear usuario**.
4. Especifique la información del usuario nuevo.
5. Si el usuario nuevo es un administrador, seleccione la opción **Admin**.
6. Pulse **Crear usuario**.

Edición de los valores de usuario

Cambie los valores de un usuario local en Master Console, como por ejemplo las contraseñas de usuario.

Acerca de esta tarea

Importante: No puede cambiar contraseñas de LDAP y Active Directory en Master Console.

Procedimiento

1. Pulse los valores ( ).
2. Pulse **Gestión de usuarios**
3. En la tarjeta del usuario que desea editar, pulse el icono de menú en la esquina superior derecha.
4. Seleccione **Editar usuario**.
5. Modifique la información de usuario en la ventana **Editar usuario**.

6. Pulse **Editar usuario** para guardar los cambios.

Eliminación de un usuario local

Elimine un usuario local de Master Console si el usuario ya no necesita acceso.

Procedimiento

1. Pulse los valores ( ).
2. Pulse la tarjeta **Gestión de usuarios** para ver las tarjetas de todos los usuarios locales.
3. En la tarjeta del usuario que desea editar, pulse el icono de menú en la esquina superior derecha.
4. Seleccione **Eliminar usuario**.
5. Pulse **Eliminar usuario** en la ventana de confirmación.

Configuración de la autenticación de Active Directory y LDAP en Master Console

Si desea utilizar Active Directory o un proveedor LDAP para la autenticación en Master Console, debe editar manualmente el archivo `/opt/qradar/masterconsole/conf/shiro.ini`.

Antes de empezar

Haga una copia de seguridad del archivo `/opt/qradar/masterconsole/conf/shiro.ini`.

Procedimiento

1. Abra el archivo `/opt/qradar/masterconsole/conf/shiro.ini`.
2. Si desea configurar Active Directory, siga estos pasos:
   a. Busque la sección siguiente:

```
# ----------------------------------------------------------------------------
# following section is for configuring ActiveDirectory realm. Replace example
# values before add to securityManager.realm
# ----------------------------------------------------------------------------
adRealm = org.apache.shiro.realm.activedirectory.ActiveDirectoryRealm
adRealm.url = ldap://{ad_server}:389
adRealm.groupRolesMap = "CN=the_users,CN=Users,DC=department,DC=company,DC=com":"admin"
adRealm.searchBase = "DC=department,DC=company,DC=com"
adRealm.systemUsername= user_name
adRealm.systemPassword= password
adRealm.principalSuffix= @company.com
```

Tabla 4. Descripciones de parámetros

Parámetro	Descripción
`searchBase`	La raíz del directorio de Active Directory o LDAP en el que se han organizado los usuarios.
`searchFilter`	Se utiliza para buscar el contexto del usuario de Active Directory o LDAP. La cuentas es una clase de objeto predeterminado utilizado para la mayoría de servidores, sin embargo esta entrada puede variar en función de la configuración del servidor Active Directory o LDAP.

Tabla 4. Descripciones de parámetros (continuación)

Parámetro	Descripción
groupAttribute	Identifica los usuarios de grupo al que el usuario de Active Directory o LDAP pertenece.
groupRolesMap	Una correlación de los grupos de Active Directory o LDAP con los roles de Shireo.
userDnTemplate	La plantilla de DN que recupera un usuario del servidor Active Directory o LDAP.
contextFactory.url	La dirección IP y el número de puerto del servidor Active Directory o LDAP.

b. Añada `$adRealm` a la entrada `securityManager.realms`:

```
securityManager.realms = $localRealm, $adRealm
```

3. Si desea configurar LDAP, siga estos pasos:
   a. Busque la sección siguiente:

```
#----------------------------------------------------------------------------
# following section is for configuring OpenLdap realm. Replace example
# values before add to securityManager.realm
#----------------------------------------------------------------------------
ldapRealm = com.ibm.si.mc.security.shiro.realm.LdapRealm
ldapRealm.searchBase = "dc=company,dc=com"
ldapRealm.searchFilter = (&(objectClass=account)(uid={0}))
ldapRealm.groupAttribute = ou
ldapRealm.groupRolesMap = "Manager":"admin"
ldapRealm.userDnTemplate = uid={0},dc=company,dc=com
ldapRealm.contextFactory.url = ldap://{ldap_server}:389
```

   b. Añada `$ldapRealm` a la entrada `securityManager.realms`:

```
securityManager.realms = $localRealm, $ldapRealm
```

4. Guarde el archivo `/opt/qradar/masterconsole/configurations/shiro.ini`.
5. Reinicie el servidor tomcat mediante el mandato siguiente:

```
service tomcat restart
```

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en Estados Unidos.

Es posible que IBM no ofrezca en otros países los productos, servicios o características que se describen en este documento. Póngase en contacto con el representante local de IBM, que le informará sobre los productos y servicios disponibles actualmente en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende indicar ni implicar que solo pueda utilizarse dicho producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente en tramitación que abarquen la materia descrita en este documento. La posesión de este documento no le confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 EE. UU.

Para consultas sobre licencias en las que se solicite información sobre el juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de Propiedad intelectual de IBM de su país o envíe las consultas, 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 es aplicable en el Reino Unido ni en ningún otro país en el que tales disposiciones sean incompatibles con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIABILIDAD O IDONEIDAD PARA UN FIN DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícita ni explícita, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no sea aplicable en su caso.

Esta información podría incluir imprecisiones técnicas o errores tipográficos. Periódicamente se realizan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras o cambios en los productos o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Las referencias hechas en esta publicación a sitios web que no son de IBM se proporcionan sólo para la comodidad del usuario y no constituyen un aval de estos sitios web. El contenido de esos sitios web no forma parte del contenido de este producto de IBM, por lo que la utilización de dichos sitios es responsabilidad del usuario.

IBM puede utilizar o distribuir la información que se le proporcione del modo que estime apropiado sin incurrir por ello en ninguna obligación con el remitente.

Los titulares de licencias de este programa que deseen obtener información sobre el mismo con el fin de permitir:(i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se haya intercambiado, deberán ponerse en contacto con:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, EE. UU.

Esta información puede estar disponible, sujeta a los términos y condiciones adecuados, incluido, en algunos casos, el pago de una tarifa.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para el mismo bajo los términos del contrato de cliente IBM, el contrato internacional de licencia de programa de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento incluidos en este documento se han obtenido en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Algunas mediciones pueden haberse realizado en sistemas en nivel de desarrollo y no existe garantía alguna de que estas mediciones sean iguales en los sistemas de disponibilidad general. Además, es posible que algunas mediciones se hayan calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para su entorno específico.

La información relacionada con productos que no son de IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, compatibilidad o cualquier otra declaración relacionada con los productos que no son de IBM. Las preguntas relativas a las prestaciones de los productos que no son de IBM deberán dirigirse a los proveedores de dichos productos.

Todas las declaraciones relativas a la orientación o intención futura de IBM están sujetas a cambio o anulación sin previo aviso y representan solamente metas y objetivos.

Todos los precios de IBM mostrados son precios de venta al público sugeridos por IBM, son actuales y están sujetos a cambio sin previo aviso. Los precios de los distribuidores pueden variar.

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales cotidianas. Para ilustrarlos de la manera más completa posible, los ejemplos incluyen los nombres de personas, empresas, marcas y productos. Todos

esos nombres son ficticios y cualquier similitud con los nombres y direcciones utilizados por empresas reales es mera coincidencia.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras empresas. Hay disponible una lista actual de marcas registradas de IBM en la web, en sección "Copyright and trademark information" de www.ibm.com/legal/copytrade.shtml.

Otros nombres de empresas, productos o servicios pueden ser marcas registradas o marcas de servicio de terceros.

Consideraciones sobre la política de privacidad

Los productos de software de IBM, incluido el software que se ofrece como soluciones de servicio (“Ofertas de software”) pueden utilizar cookies u otras tecnologías para recopilar información sobre la utilización del producto a fin de mejorar la experiencia final del usuario, personalizar las interacciones con el usuario final o para otros fines. En muchos casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras Ofertas de software pueden ayudarle a recopilar información de identificación personal. Si esta Oferta de software utiliza cookies para recopilar información de identificación personal, más adelante se proporciona información específica sobre el uso de cookies por parte de la oferta de software.

En función de las configuraciones desplegadas, esta Oferta de software puede utilizar cookies de sesión que recopilan el ID de sesión de cada usuario para la gestión y autenticación de sesiones. Estas cookies se pueden inhabilitar, pero si se inhabilitan también se elimina la función que estas cookies habilitan.

Si las configuraciones desplegadas para esta Oferta de software le ofrecen como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento jurídico sobre la legislación aplicable a esa recopilación de datos, que incluye cualquier requisito de aviso y consentimiento.

Para obtener más información sobre el uso de diversas tecnologías, incluidas las cookies, para estos fines, consulte la política de privacidad de IBM en http://www.ibm.com/privacy y la declaración de privacidad en línea de IBM en http://www.ibm.com/privacy/details, la sección titulada “Cookies, Web Beacons and Other Technologies” y la declaración “IBM Software Products and Software-as-a-Service Privacy Statement” en http://www.ibm.com/software/info/product-privacy.

Impreso en España