Contenido

Guía de inicio rápido de IBM Data Risk Manager

Guía de inicio rápido

Versión 2.0.6

Esta guía describe una forma fácil y rápida para instalar y configurar IBM Data Risk Manager.

Nota:

Acerca de esta tarea

Visión general del producto

Puede utilizar IBM Data Risk Manager para descubrir, analizar, clasificar, supervisar y visualizar los activos empresariales y los riesgos que están asociados a datos confidenciales. IBM Data Risk Manager proporciona las prestaciones siguientes:

- Un proceso programático para el descubrimiento continuo, la clasificación y la creación de informes de datos confidenciales y los riesgos asociados en toda la empresa.
- Un proceso sostenible y eficiente asistido por automatización para proporcionar vistas de riesgos empresariales en tiempo real.
- Una asociación de activos con metadatos empresariales como, por ejemplo, procesos empresariales, aplicaciones y partes interesadas.

IBM Data Risk Manager está formado por distintos módulos de aplicación como, por ejemplo, el Modelador de contexto empresarial (BCM), el Centro de control y mandatos de seguridad (SC3) y el panel de control de Data Risk Manager.

Procedimiento

1. Acceder al software

   IBM Data Risk Manager se distribuye como un dispositivo virtual de software preconfigurado. El dispositivo virtual proporciona todo el entorno de software para la instalación de Data Risk Manager que incluye el sistema operativo guardado. La imagen está en el formato de archivo Open Virtual Appliance (.ova) y tiene como objetivo desplegarse en una máquina virtual.

   Puede descargar IBM Data Risk Manager, Versión 2.0.6 desde el sitio web de IBM Passport Advantage en http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm en forma de paquetes eAssembly para los sistemas operativos soportados. Para obtener más información, consulte la sección "Instrucciones de descarga de software" en la documentación de IBM Data Risk Manager (https://www.ibm.com/support/knowledgecenter/SSJQ6V_2.0.6/com.ibm.idrm.doc/admin/top/cpt_admin_download.html).

   El paquete de IBM Data Risk Manager incluye las ofertas siguientes:

   - Imagen Open Virtual Appliance (ova) de IBM Data Risk Manager
   - Guía de inicio rápido de producto

Para obtener una documentación completa, incluidas las instrucciones de instalación, consulte la documentación de IBM Data Risk Manager (https://www.ibm.com/support/knowledgecenter/SSJQ6V_2.0.6/com.ibm.idrm.doc/welcome.html).

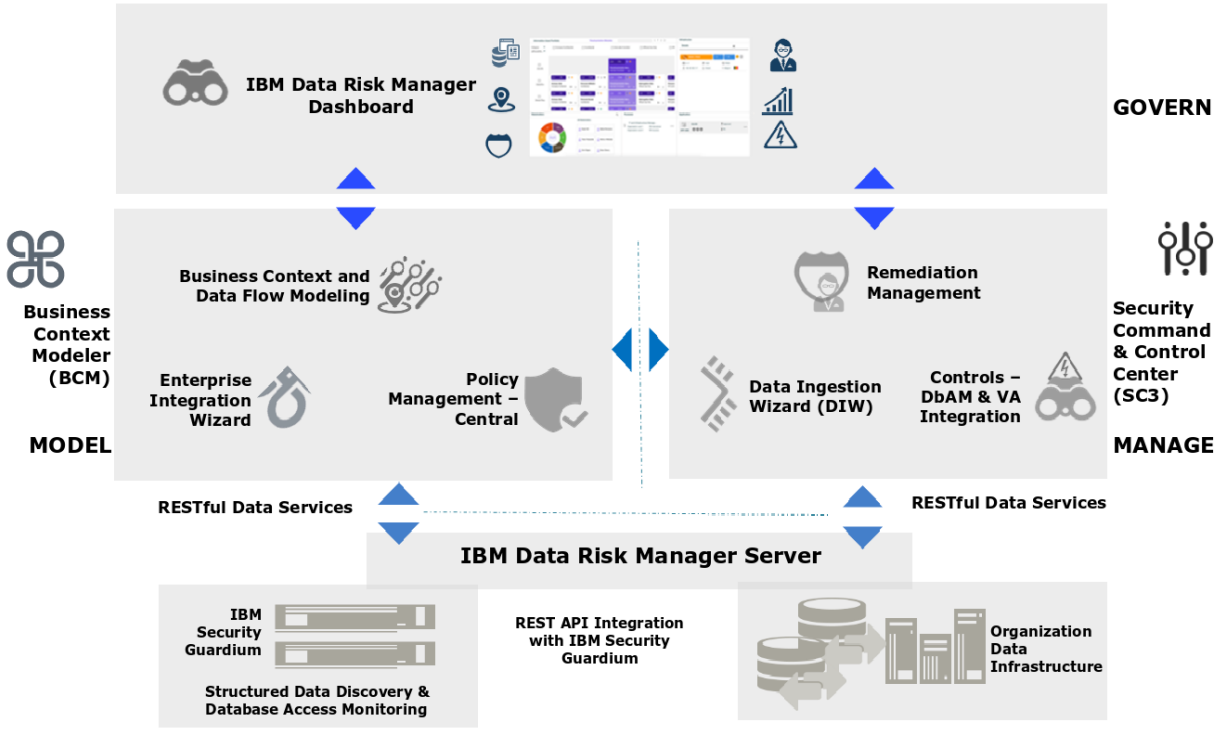
El IBM Data Risk Manager incluye determinado software de Red Hat, que está sujeto a los acuerdos de licencia que se pueden visualizar a través de: http://www-03.ibm.com/software/sla/sladb.nsf/displaylis/20E0A31663D6F996852581E500480032?OpenDocument

2. Evaluar la configuración del sistema y del hardware

   Para obtener información sobre los requisitos del sistema y los sistemas operativos soportados, consulte la sección "Instalación y configuración" de la documentación de IBM Data Risk Manager (https://www.ibm.com/support/knowledgecenter/SSJQ6V_2.0.6/com.ibm.idrm.doc/install/top/landing-install.html).

3. Revisión de la arquitectura funcional

   La arquitectura funcional siguiente ilustra distintos módulos y submódulos de IBM Data Risk Manager. Los módulos funcionales de IBM Data Risk Manager se agrupan para permitir a las empresas modelar sus datos de contexto empresarial con el Modelador de contexto empresarial, gestionar a través del Centro de control y mandatos de seguridad y controlar con el panel de control de IBM Data Risk Manager.



4. Instalar IBM Data Risk Manager

   Planificación de la instalación e importación de dispositivo virtual

   La máquina virtual IBM Data Risk Manager es de suministro ligero de forma predeterminada con 200 GB de almacenamiento. En función de sus requisitos de negocio, puede modificar el uso de la CPU, la memoria y la capacidad del disco duro.

   Para obtener más información sobre la instalación, consulte la sección "Instalación y configuración" de la documentación de IBM Data Risk Manager (https://www.ibm.com/support/knowledgecenter/SSJQ6V_2.0.6/com.ibm.idrm.doc/install/top/landing-install.html).

5. Configurar

   La configuración de IBM Data Risk Manager se describe en la sección "Instalación y configuración" de la documentación de IBM Data Risk Manager (https://www.ibm.com/support/knowledgecenter/SSJQ6V_2.0.6/com.ibm.idrm.doc/install/top/landing-install.html).

Para obtener información de resolución de problemas de IBM Data Risk Manager, consulte la sección "Resolución de problemas y soporte" en la documentación (https://www.ibm.com/support/knowledgecenter/SSJQ6V_2.0.6/com.ibm.idrm.doc/trouble/top/landing_trouble.html).

Qué hacer a continuación
Más información

Para obtener más información, consulte el soporte del producto IBM Data Risk Manager en http://www-947.ibm.com/support/entry/portal/overview/software/software_support_(general).

Instrucciones de descarga de software

Puede obtener las imágenes de instalación descargables para IBM Data Risk Manager desde el sitio web de IBM Passport Advantage.

Utilice el sitio web de IBM Passport Advantage en http://www-01.ibm.com/software/lotus/passportadvantage/pao_customer.html para adquirir IBM Data Risk Manager. Puede descargar o solicitar un paquete de soporte del software autorizado.

El sitio web de IBM Passport Advantage proporciona paquetes, llamados eAssemblies, para los productos IBM.

El sitio web de Fix Central proporciona arreglos y actualizaciones para el software, hardware y sistema operativo del sistema. Los fixpacks de IBM Data Risk Manager se publican en el sitio web de http://www.ibm.com/support/fixcentral.

La sección “Instalación y configuración” en IBM Knowledge Center para IBM Data Risk Manager proporciona instrucciones para descargar, instalar y configurar IBM Data Risk Manager.

Imágenes de instalación de IBM Data Risk Manager

IBM Data Risk Manager proporciona imágenes de instalación descargables.

Ejecute los pasos siguientes para extraer paquetes de eImage:

1. Descargue el paquete de eImage que necesite. El paquete de eImage se describe en la tabla siguiente.

   Puede descargar el paquete de eImage desde el sitio web de IBM Passport Advantage en: http://www-01.ibm.com/software/lotus/passportadvantage/pao_customer.html
2. Desempaquete el paquete de eImage en un directorio temporal en el sistema.
3. Seleccione un directorio temporal diferente para utilizar como directorio base para la instalación.
4. Siga las instrucciones en la sección “Instalación y configuración” en IBM Knowledge Center para IBM Data Risk Manager para instalar el producto.

eImage	Descripción
CC4FREN	eImage para IBM Data Risk Manager, Versión 2.6.

Visión general del producto

La visión general del producto contiene temas que describen los conceptos principales y otra información importante para ayudarle a utilizar el sistema.

Novedades de este release

Descripción de las características y otra información específica del release actual de IBM Data Risk Manager.

Intercambio de integración

IBM Data Risk Manager soporta ahora la integración con los siguientes productos.

IBM StoredIQ
Puede integrar IBM Data Risk Manager con IBM StoredIQ para importar el inventario del descubrimiento de datos no estructurados para el análisis de riesgos y acciones. Para obtener más información sobre la integración, consulte “Integración de IBM StoredIQ con IBM Data Risk Manager” en la página 92.

ServiceNow
Puede utilizar la integración de IBM Data Risk Manager y ServiceNow para crear, actualizar y cerrar incidencias de ServiceNow para las actividades de reparación que se han creado en el Centro de acción. Para obtener más información sobre la integración, consulte “Integración de ServiceNow con IBM Data Risk Manager” en la página 73.

Editor del registro

Además de cargar los archivos CSV para la correlación de datos de contexto, también puede utilizar el editor del registro para correlacionar datos de contexto. Puede utilizar el componente Gestionar inventario para ver y gestionar datos de contexto empresarial. Para obtener más información sobre este nuevo flujo de trabajo, consulte “Gestión de inventario ” en la página 113.

Vista de residencia de aplicación - Privacy Splash

El widget Distribución geográfica de activos de información en la página Privacy Splash de IBM Data Risk Manager ahora muestra las ubicaciones del servidor de aplicaciones en un mapa global. Para obtener más información sobre la vista de residencia de aplicación, consulte “Distribución geográfica de los activos de información” en la página 173.

Mejoras del Centro de acción

Ahora puede utilizar la integración de IBM Data Risk Manager y ServiceNow para crear, actualizar y cerrar incidencias de ServiceNow para las actividades de reparación que se crean en el Centro de acción. Asimismo, también hay mejoras en el Centro de acción para la gestión de flujo de trabajo. Para obtener más información sobre el Centro de acción, consulte “Centro de acción” en la página 151.

Evaluación de la puntuación de riesgo

Ahora se utilizan distintos vectores para evaluar automáticamente los riesgos de activo de información. Para obtener más información sobre la evaluación de la puntuación de riesgo, consulte “Modelado y visualización de riesgos” en la página 169.

Mejoras en el panel de control de IBM Data Risk Manager

El panel de control de IBM Data Risk Manager proporciona una visión más amplia de los riesgos de datos que están asociados a una infraestructura del activo de información. Para obtener más información sobre el panel de control, consulte “Panel de control de IBM Data Risk Manager” en la página 177.

Gestión de resultados de evaluación

Basándose en los resultados de la evaluación no PRA, se deben implementar las acciones apropiadas para abordar y mitigar los riesgos identificados. Puede utilizar el módulo Gestión del resultado de evaluación de IBM Data Risk Manager para ver y gestionar los riesgos. Para obtener más información sobre la gestión por resultados, consulte “Gestión de resultados de evaluación” en la página 201.

Exportación de orígenes de datos limpios al panel de control

Puede exportar directamente los orígenes de datos de IBM Security Guardium limpios al panel de control de IBM Data Risk Manager. Para obtener más información, consulte “Exportación de orígenes de datos IBM Security Guardium limpios al panel de control ” en la página 49.

Introducción a IBM Data Risk Manager

IBM Data Risk Manager proporciona a los líderes de negocio un centro de control de riesgos de datos de consumo empresarial que permite descubrir, analizar y visualizar los riesgos empresariales relacionados con los datos. A continuación, los líderes de negocio pueden abordar de forma proactiva los riesgos empresariales relacionados con los datos para proteger sus organizaciones.

IBM Data Risk Manager proporciona respuestas a las preguntas siguientes sobre riesgos de datos.

- ¿Qué datos son más críticos?
- ¿Dónde están ubicados los datos críticos? y ¿están protegidos?
- ¿Quiénes son los propietarios de los datos críticos?
- ¿Quién accede a los datos críticos?
- ¿Cómo se exponen los datos a riesgos de seguridad?
- ¿Sobre quién recae la responsabilidad si los datos están expuestos?
- ¿Cuáles son las medidas adecuadas que se deben adoptar en función de la importancia de los datos?

Problemas de protección de datos

Los activos de información confidenciales sobre la empresa de una organización están formados por información de clientes, propiedad intelectual, información de empleados, planes de fusión y adquisición, información financiera, estrategia de ventas, etc. Los procesos empresariales necesitan y utilizan estos activos de información en toda la organización y dependen de su disponibilidad e integridad para completar sus operaciones. En algunos casos, estos activos de información constituyen la base de la diferenciación competitiva y ofrecen una ventaja en el mercado.

Obtener una comprensión de los tipos de activos confidenciales, su valor para la organización, cómo están protegidos y los requisitos de conformidad que se aplican a la información son fundamentales para tomar decisiones estratégicas y aplicar los controles adecuados.

Esto podría parecer un enorme esfuerzo y muchas organizaciones podrían sentirse renuentes a emprender este trayecto. La organización podría enfrentar los siguientes retos:

- Necesidad de descubrir activos de información confidencial y almacenes de datos aún sin identificar en una ventana temporal limitada.
- Comprender el acceso a datos confidenciales, la actividad y sus flujos para determinar las amenazas, las exposiciones y las vulnerabilidades.
- Determinar los riesgos empresariales asociados a los activos de información e identificar y priorizar la implementación de controles.
- Demostrar la conformidad con los nuevos requisitos de mandatos reglamentarios y corporativos que se hayan incorporado y la auditoría interna.
- Reducir el coste y la complejidad del despliegue y la gestión de las soluciones de supervisión.

IBM Data Risk Manager proporciona a las empresas las prestaciones siguientes.

Descubrir
: Descubrir bases de datos y aplicaciones que contienen datos cruciales de la organización.

Analizar
: Proporciona información sobre los riesgos potenciales que pueden afectar a la información confidencial sobre la empresa.

Visualizar
: Proporciona al equipo ejecutivo la visibilidad de sus datos críticos.

Actuar
Crea procesos sostenibles, asequibles y vigentes para ayudar a gestionar los activos críticos y los riesgos de forma eficaz.

Características principales de IBM Data Risk Manager

Centro de control de riesgos de datos interactivo
Visualice y gestione los datos en una vista unificadora de un solo panel que permite transmitir valor y significado a los ejecutivos empresariales. Correlacione las métricas de seguridad de las soluciones de seguridad puntuales para proporcionar una vista integral de su posición de seguridad, utilizando el lenguaje común de riesgo para comunicarse con la suite C y la oficina de riesgo.

Descubrimiento de datos y clasificación
Descubra, clasifique e informe programáticamente los datos confidenciales y los riesgos asociados en toda la empresa integrando las salidas de diversos productos de software. Utiliza información en tiempo real para descubrir de forma eficaz activos de información confidenciales y almacenes de datos todavía sin identificar.

Analítica automatizada
Analice los riesgos identificados, su tipo, los activos de información afectados y los elementos adicionales para ofrecer una visión completa de su potencial de probabilidad y de impacto empresarial. Basándose en la analítica, elija las acciones de mitigación que permiten impedir sufrir pérdidas de información.

Modelado y evaluación de riesgos empresariales
Correlacionar amenazas, vulnerabilidades, controles y atributos de negocio con el valor del activo de información. Calcular una puntuación de riesgo que resalta las partes de la empresa que están en riesgo.

Beneficios clave de utilizar IBM Data Risk Manager

- Proporciona una visibilidad anticipada de los riesgos potenciales que pueden afectar a los activos y procesos de información empresarial confidenciales.
- Identifica activos de información confidencial empresarial y de alto valor específicos que están en riesgo debido a amenazas internas o externas.
- Proporciona una vista completa de los metadatos empresariales asociada a los datos confidenciales para los elementos siguientes.
  - Aplicaciones
  - Procesos
  - Política y procedimientos
  - Controles y propiedad
- Ofrece valor y significado a los directivos de empresa con un panel de control exclusivo y fácil de entender.
- Habilita las conversaciones correctas con equipos de TI, de seguridad y de línea de negocio (LOB) para mejorar los procesos empresariales y mitigar los riesgos.
- Permite tomar medidas proactivas para evitar impactos potenciales y evitar pérdidas.

Componentes de IBM Data Risk Manager

IBM Data Risk Manager contiene varios componentes que trabajan conjuntamente para descubrir, analizar, clasificar, supervisar y visualizar activos y riesgos empresariales.

IBM Data Risk Manager incluye los componentes siguientes.

Panel de control de IBM Data Risk Manager
Proporciona visualización y gestión de datos en una vista unificadora de un solo panel que permite transmitir valor y significado a los directivos de la empresa. Un panel de control interactivo que permite el control de información gracias a la visualización y gestión en una única consola unificadora que representa los riesgos potenciales para los activos confidenciales de la empresa.

- Proporciona una visualización interactiva de la cartera de activos de información, la clasificación de datos y los requisitos de seguridad.
- Permite la aplicación de controles de seguridad proactivos y la mitigación de riesgos al proporcionar visibilidad de riesgos potenciales, exposiciones y vulnerabilidades.
- Combina activos de información, procesos y metadatos de controles para representar la seguridad de datos y la posición de control.
- Habilita el control de información que permite a los líderes de negocio visualizar los riesgos en los activos confidenciales en todas las funciones de negocio y ayuda a comprender la posible repercusión en la organización.
- Proporciona supervisión de conformidad a través de notificaciones en tiempo real y elementos de acción en alineación con las políticas y requisitos de seguridad de datos.

Modelador de contexto empresarial (BCM)
Modela el flujo de elementos de datos en toda la organización intercalando entidades y participantes que incluyen procesos empresariales, aplicaciones, nodos de infraestructura y especificación de control.

- Define el contexto de descubrimiento recopilando y modelando la información necesaria para el descubrimiento de datos confidenciales.
  - Entorno de infraestructura como, por ejemplo, topología de red, arquitectura de aplicaciones y repositorios de datos.
  - Información de metadatos necesaria para configurar la infraestructura de descubrimiento y la planificación de exploraciones de descubrimiento.
  - Políticas de descubrimiento dado que son relevantes para los objetivos de descubrimiento respectivos.
- Proporciona una representación visual de los elementos de datos descubiertos y su flujo en todas las entidades organizativas.
- Utiliza herramientas de la empresa existentes para recopilar información pertinente para el descubrimiento y el modelado de flujos de datos.

Centro de control y mandatos de seguridad (SC3)
Proporciona una solución de gestión de descubrimiento de datos que habilita las definiciones de políticas de descubrimiento de datos, el descubrimiento de datos, el análisis y la limpieza de datos descubiertos, la categorización de activos de información y la gestión de reparaciones.

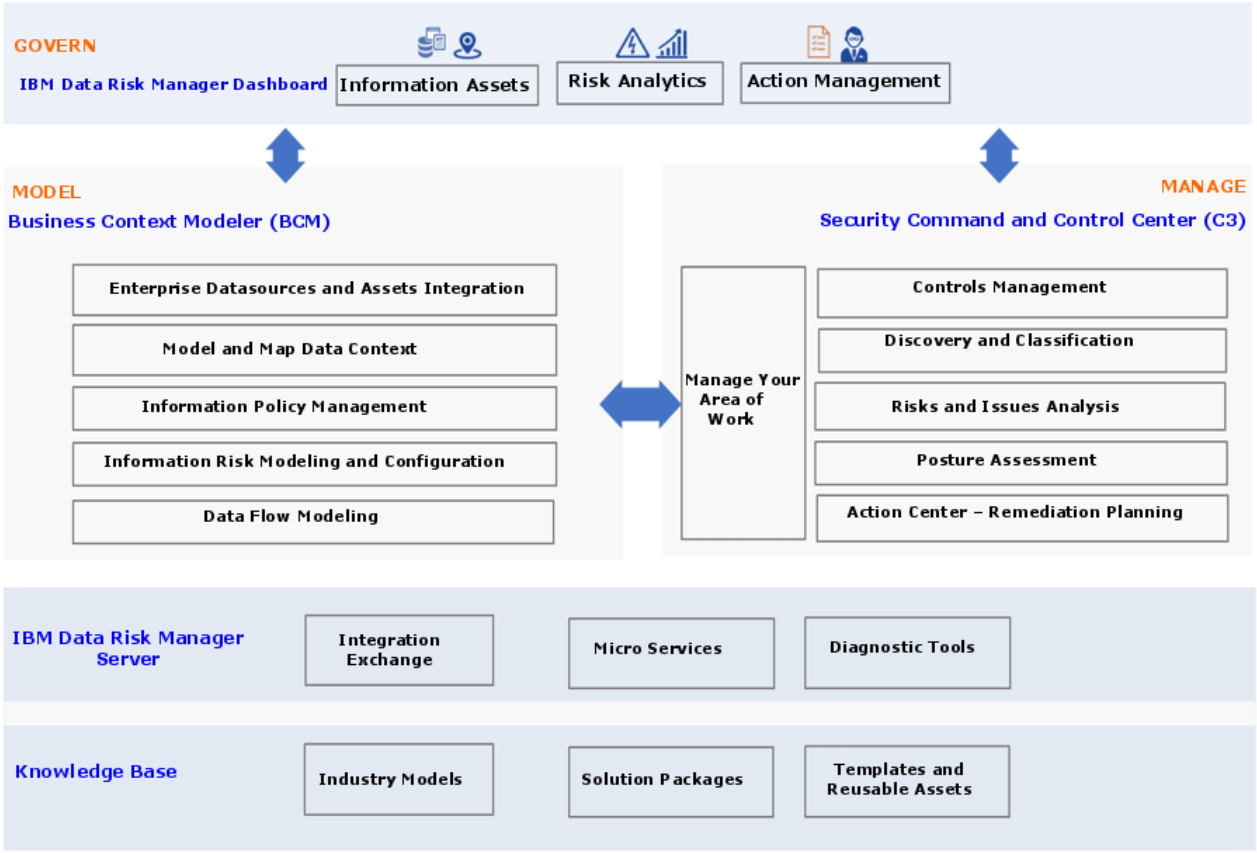
- Define políticas de descubrimiento y reglas de clasificación para desplegarlas en IBM Security Guardium y habilita la sincronización de políticas.
- Facilita la planificación de exploración mediante el análisis y la consolidación de inventario de objetivos de descubrimiento.
- Permite el descubrimiento delta continuo identificando automáticamente los cambios en el inventario de los objetivos y el esquema de descubrimiento.
- Repositorio de criterios de descubrimiento y clasificación, políticas de descubrimiento y supervisión, amenazas y vulnerabilidades que se basan en los estándares del sector.
- Proporciona visibilidad de los activos de información críticos de la empresa, agrupándolos según una taxonomía preconfigurada basada en los criterios de clasificación.

Servidor de IBM Data Risk Manager
El componente de servidor de IBM Data Risk Manager.

Arquitectura funcional de IBM Data Risk Manager

La arquitectura de IBM Data Risk Manager incluye los componentes de Modelador de contexto empresarial (BCM), Centro de control y mandatos de seguridad (SC3), panel de control de IBM Data Risk Manager y servidor de aplicaciones de Data Risk Manager para descubrir, analizar, clasificar, supervisar y visualizar los activos y riesgos empresariales.

El diagrama siguiente ilustra la arquitectura funcional de IBM Data Risk Manager.



La arquitectura de IBM Data Risk Manager incluye los siguientes grupos funcionales.

Modelo

Representa las funciones asociadas a la instalación, configuración y alineación de IBM Data Risk Manager con el contexto de la organización.

Modelado de flujo de datos

Habilita la correlación visual del flujo de activos de datos dentro de la organización entre entidades empresariales y de infraestructura.

Central de gestión de políticas

Crea y gestiona las políticas de IBM Data Risk Manager.

Asistente de integración empresarial (EIW)

Incluye todas las funciones relacionadas con la integración con sistemas empresariales y la importación de repositorios u otros metadatos de la organización. Las funciones de EIW incluyen `User`, `User Group`, `Integration`, `Organization`, `A3 Repo`, `Native Discovery` y `Manage Inventory`.

Creador de infraestructuras

El grupo funcional Modelo incluye el componente WebSphere Business Modeler de contexto empresarial de IBM Data Risk Manager.

Gestionar

Representa las funciones operativas y diarias de IBM Data Risk Manager..

Asistente de ingesta de datos (DIW)

Habilita el descubrimiento, las clasificaciones, el análisis y la asignación de taxonomía de los datos confidenciales de las organizaciones.

Gestión de reparaciones (Centro de acción)

Define y gestiona los flujos de trabajo del producto que incluyen elementos de acción, tareas y asignaciones de partes interesadas. Los flujos de trabajo se utilizan para gestionar programas de seguridad de datos y para reparar problemas y riesgos.

Controles: supervisión de actividad de base de datos (DAM) y evaluación de vulnerabilidades (VA)
Asociados a la integración de IBM Data Risk Manager con las prestaciones de DAM y VA de IBM Security Guardium.

El grupo funcional de gestión incluye el componente SC3 de IBM Data Risk Manager.

Controlar
Habilita el gobierno proporcionando visibilidad de activos de datos de las organizaciones, tipos de activos confidenciales y su valor a la organización, cómo se protegen los activos de datos y qué requisitos de conformidad se aplican a la información para tomar decisiones estratégicas. El grupo funcional Controlar incluye el componente de panel de control de IBM Data Risk Manager.

Aceleradores de integración

IBM Data Risk Manager se puede utilizar con otros productos de seguridad para obtener una solución integrada.

IBM Data Risk Manager se puede integrar con los productos siguientes que ofrecen un proceso programático para el descubrimiento continuo, la clasificación y la creación de informes de datos confidenciales, así como los riesgos asociados en toda la empresa.

- IBM Security Guardium
- IBM Security AppScan Enterprise
- DLP de Symantec
- IBM InfoSphere Information Governance Catalog
- IBM QRadar Security Intelligence Platform
- ServiceNow
- Imperva SecureSphere
- IBM Multi-Cloud Data Encryption
- OneTrust
- IBM Security Guardium Analyzer
- IBM StoredIQ

Versiones soportadas

Producto	Versión
IBM Security Guardium	10.5, 10.6 y 11.0
IBM Security AppScan Enterprise	9.0.3.8
DLP de Symantec	12.x y 14.x
IBM QRadar Security Intelligence Platform	7.3.1
IBM InfoSphere Information Governance Catalog	11.5 y 11.7
Imperva SecureSphere	13.0.0.10
IBM Multi-Cloud Data Encryption	2.2
OneTrust	NA
IBM Security Guardium Analyzer	NA
IBM StoredIQ	7.6.0.19

Integración con IBM Security Guardium
Configure IBM Data Risk Manager para que se comunique con IBM Security Guardium y utilizar la información de riesgo relacionada con los datos confidenciales en IBM Data Risk Manager para el análisis de riesgos.

IBM Security Guardium está diseñado para ayudar a proteger los datos críticos. IBM Security Guardium ayuda a garantizar la integridad de la información en los centros de datos y a automatizar los controles de conformidad. Para obtener más información sobre IBM Security Guardium, consulte la documentación del producto en la documentación de IBM Security Guardium.

Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium con IBM Data Risk Manager" en la página 34.

Integración con IBM Security AppScan Enterprise
Configure IBM Data Risk Manager para que se comunique con IBM Security AppScan Enterprise para utilizar su información de riesgo confidencial en IBM Data Risk Manager para evaluaciones.

IBM Security AppScan Enterprise permite a las organizaciones mitigar los riesgos de seguridad de las aplicaciones, reforzar las iniciativas de gestión de programas de seguridad de aplicaciones y obtener la conformidad con la normativa. Los equipos de desarrollo y seguridad pueden colaborar, establecer políticas y escalar las pruebas en todo el ciclo de vida de las aplicaciones. Para obtener más información sobre IBM Security AppScan Enterprise, consulte la documentación del producto en Documentación de IBM Security AppScan Enterprise .

Para obtener más información sobre la integración, consulte "Integración de IBM Security AppScan Enterprise con IBM Data Risk Manager" en la página 60.

Integración con DLP de Symantec
Configure IBM Data Risk Manager para comunicarse con la conexión DLP (Data Loss Prevention) de Symantec para importar incidencias y políticas de DLP de Symantec Versión 12.x y 14.x a IBM Data Risk Manager.

Symantec Data Loss Prevention (DLP de Symantec) es una tecnología de seguridad basada en el contenido que permite a las empresas comprender dónde se almacena la información corporativa confidencial, cómo se utilizan los datos y cómo proteger los datos frente a la pérdida y el robo.

Para obtener más información sobre la integración, consulte "Integración de DLP de Symantec con IBM Data Risk Manager" en la página 68.

Integración con IBM InfoSphere Information Governance Catalog
Configure IBM Data Risk Manager para que se comunique con IBM InfoSphere Information Governance Catalog para importar los metadatos en IBM Data Risk Manager.

IBM InfoSphere Information Governance Catalog es una herramienta interactiva, basada en web que permite a los usuarios crear, gestionar y compartir vocabulario empresarial y un sistema de clasificación en un catálogo central. IBM InfoSphere Information Governance Catalog ayuda a los usuarios a comprender el significado empresarial de sus activos y proporciona funciones de búsqueda, navegación y consulta. Para obtener más información acerca de IBM InfoSphere Information Governance Catalog, consulte la documentación del producto.

Para obtener más información sobre la integración, consulte "Integración de IBM InfoSphere Information Governance Catalog con IBM Data Risk Manager" en la página 75.

Integración con IBM QRadar Security Intelligence Platform
Configure IBM Data Risk Manager para que se comunique con IBM QRadar Security Intelligence Platform, Versión 7.3.1, para utilizar su información de riesgo relacionada con datos confidenciales en IBM Data Risk Manager.

Los productos de IBM QRadar Security Intelligence Platform proporcionan una arquitectura unificada para integrar la gestión de sucesos e información de seguridad (SIEM), la gestión de registros, la detección de anomalías, los estudios forenses de incidentes y la gestión de la configuración y de vulnerabilidades. Para obtener más información sobre IBM QRadar Security Intelligence Platform,

consulte la documentación del producto en Documentación de IBM QRadar Security Intelligence Platform.

Para obtener más información sobre la integración, consulte Integración de IBM QRadar Security Intelligence Platform Adapter.

Integración con ServiceNow
Configure IBM Data Risk Manager para que se conecte e interactúe con ServiceNow para importar información de taxonomía y datos de topología de red en IBM Data Risk Manager.

Para obtener más información sobre la integración, consulte "Integración de ServiceNow con IBM Data Risk Manager" en la página 73.

Integración con Imperva SecureSphere
Configure IBM Data Risk Manager para que se conecte e interactúe con Imperva SecureSphere para importar información de vulnerabilidad en IBM Data Risk Manager.

Para obtener más información acerca de Imperva SecureSphere, consulte la documentación del producto.

Para obtener más información sobre la integración, consulte "Integración de Imperva SecureSphere con IBM Data Risk Manager" en la página 80.

Integración con IBM Multi-Cloud Data Encryption
Configure IBM Data Risk Manager para conectarse e interactuar con IBM Multi-Cloud Data Encryption para captar detalles de cifrado de orígenes de datos añadidos al inventario de distintos orígenes donde está desplegado el agente de IBM Multi-Cloud Data Encryption para el cifrado de datos.

Para obtener más información acerca de IBM Multi-Cloud Data Encryption, consulte la documentación del producto.

Para obtener más información sobre la integración, consulte "Integración de IBM Multi-Cloud Data Encryption con IBM Data Risk Manager" en la página 83.

Integración con OneTrust
Configure IBM Data Risk Manager para conectarse e interactuar con OneTrust para importar inventarios y su información de riesgo correspondiente en IBM Data Risk Manager. Estos riesgos se correlacionan con los activos de información y la infraestructura correspondientes en IBM Data Risk Manager para visualizarlos en el panel de control para el análisis de riesgo y las acciones.

Para obtener más información acerca de OneTrust, consulte la documentación del producto.

Para obtener más información sobre la integración, consulte "Integración de OneTrust con IBM Data Risk Manager" en la página 85.

Integración con IBM Security Guardium Analyzer
Configure IBM Data Risk Manager para conectar e interactuar con IBM Security Guardium Analyzer a fin de importar exploraciones de clasificador e información de vulnerabilidad en un análisis de riesgos.

Para obtener más información acerca de IBM Security Guardium Analyzer, consulte la documentación del producto.

Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium Analyzer con IBM Data Risk Manager" en la página 88.

Integración con IBM StoredIQ
Configure IBM Data Risk Manager para conectarse con e interactuar con IBM StoredIQ para utilizar sus resultados de datos de clasificación para el análisis de riesgos y acciones.

Para obtener más información sobre IBM StoredIQ, consulte la documentación del producto en: https://www.ibm.com/support/knowledgecenter/SSSHEC_7.6.0/welcome/storediq.html

Para obtener más información sobre la integración, consulte "Integración de IBM StoredIQ con IBM Data Risk Manager" en la página 92.

Interfaz del usuario

La solución IBM Data Risk Manager tiene una consola de aplicaciones basada en la web (suite de aplicaciones) para gestionar varias funciones de descubrimiento y clasificación de datos y para ejecutar varias tareas administrativas para instalar y configurar el entorno de IBM Data Risk Manager.

Acceso a la suite de aplicaciones de IBM Data Risk Manager

Para acceder a la suite de aplicaciones de IBM Data Risk Manager, escriba la siguiente dirección web en el navegador web:

```
https://<direcciónIP-servidor-IDRM-de-su-equipo>:8443/albatross/A3Suite/
```

<direcciónIP-servidor-IDRM-de-su-equipo> es la dirección IP del servidor en el que se ha instalado IBM Data Risk Manager.

Gestión de licencias

IBM Data Risk Manager genera archivos SLMT (Software License Metric Tag) de IBM en un formato compatible con IBM License Metric Tool. IBM License Metric Tool utiliza estos archivos y genera informes de consumo de licencia.

Cada instancia de IBM Data Risk Manager genera archivos SLMT (`.slmtag`). La métrica supervisada es `MANAGED_DEVICE`, cuyo valor se registra cada vez que se exporta un activo al panel de control de IBM Data Risk Manager.

La métrica `MANAGED_DEVICE` es un nodo de infraestructura que contiene activos de información confidencial. El número total de nodos de infraestructura distintos que gestiona IBM Data Risk Manager es igual al recuento de la etiqueta value de la métrica.

Formato de archivo SLMT

Los archivos `.slmtag` se almacenan en formato XML sin ningún elemento raíz para facilitar las modificaciones. Los archivos constan de dos partes:

- Información de cabecera como, por ejemplo, `SchemaVersion` y `SoftwareIdentity`.
- Información de consumo de licencia añadida periódicamente (`MANAGED_DEVICE`).

```
<SchemaVersion>2.1.1</SchemaVersion>
<SoftwareIdentity>
    <PersistentId>b795148d68074e319e38f550050f315b</PersistentId>
    <Name>IBM Data Risk Manager Server</Name>
    <InstanceId>/home/a3user/Tomcat</InstanceId>
</SoftwareIdentity>
<Metric logTime="2018-12-03T14:37:10+05:30">
    <Type>MANAGED_DEVICE</Type>
    <SubType></SubType>
    <Value>32</Value>
    <Period>
        <StartTime>2018-12-03T14:31:25+05:30</StartTime>
        <EndTime>2018-12-03T14:37:07+05:30</EndTime>
    </Period>
</Metric>
```

La etiqueta `<Value>` indica el número de nodos de infraestructura distintos que se exportan al panel de control a la vez, que se especifica mediante `<EndTime>`.

Configuración del archivo SLMT

El archivo de etiquetas se encuentra en `/opt/ibm/slmtags` en el servidor de IBM Data Risk Manager. Cuando el tamaño de archivo `.slmtag` alcanza el límite de 100 KB predeterminado, se inicia la rotación de archivos de registro y se archiva el archivo existente.

Idiomas admitidos

IBM Data Risk Manager admite distintos idiomas. Las etiquetas, los mensajes y los valores de la interfaz de usuario (web) se pueden mostrar en inglés y en idiomas distintos del inglés.

IBM Data Risk Manager admite los idiomas siguientes:

- Inglés
- Francés
- Alemán
- Italiano
- Japonés
- Coreano
- Chino simplificado
- Español
- Chino tradicional

Información de release

Los temas de información de release proporcionan información que necesita conocer antes de instalar y utilizar el producto, tales como los requisitos de hardware y software, y problemas y limitaciones conocidos.

Problemas conocidos de IBM Data Risk Manager

Las notas del release contienen información sobre los problemas, las limitaciones y las soluciones temporales de IBM Data Risk Manager. Las notas del release se publican como una nota técnica.

Puede acceder a la nota técnica en: https://www-01.ibm.com/support/docview.wss?uid=ibm11096012

Requisitos del sistema

El entorno debe cumplir los requisitos mínimos del sistema para instalar IBM Data Risk Manager.

Para obtener más información sobre los requisitos de hardware y software, consulte la sección *Instalación y configuración* en IBM Knowledge Center para IBM Data Risk Manager. Los requisitos de hardware y software que se publican son correctos en el momento de la publicación.

Puede también consultar el documento detallado de requisitos del sistema en https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html.

1. Especifique `IBM Data Risk Manager`.
2. Seleccione la versión del producto. Por ejemplo, `2.0.6`.
3. Seleccione el sistema operativo.
4. Pulse **Enviar**.

Novedades en IBM Data Risk Manager, Versión 2.0.4

Descripción de las características y otra información específica de la versión 2.0.4 de IBM Data Risk Manager.

Informes de IBM Data Risk Manager

El motor de informes de IBM Data Risk Manager se puede usar para generar informes usando varias plantillas predefinidas para visualizar y analizar los datos con facilidad. Para obtener más información sobre los informes de IBM Data Risk Manager, consulte “Informe” en la página 156.

Planificador de IBM Data Risk Manager

Ahora puede usar la función Planificador de IBM Data Risk Manager para crear y gestionar trabajos de ejecución automática de varias transacciones en los intervalos que defina. Para obtener más información sobre el planificador de IBM Data Risk Manager, consulte "Planificador de IBM Data Risk Manager" en la página 162.

Servidores de integración

IBM Data Risk Manager soporta ahora la integración con los siguientes productos.

IBM Security Guardium Analyzer
Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium Analyzer con IBM Data Risk Manager" en la página 88.

IBM Multi-Cloud Data Encryption
Para obtener más información sobre la integración, consulte "Integración de IBM Multi-Cloud Data Encryption con IBM Data Risk Manager" en la página 83.

Imagen de pantalla de privacidad

Se puede visualizar información de privacidad y seguridad de datos en varios widgets de IBM Data Risk Manager Privacy Splash de diferentes maneras que ayudan a analizar y abordar rápidamente los riesgos de privacidad y seguridad. Para obtener más información sobre Privacy Splash, consulte "IBM Data Risk Manager Privacy Splash" en la página 173.

Evaluación basada en ámbito e informe

Durante la creación del programa de evaluación para infraestructuras no basadas en PRA, se puede definir el ámbito de la evaluación en términos de entidades de negocio o dominios como, por ejemplo, procesos de negocio, aplicaciones y activos. El uso de ámbitos en la evaluación garantiza la recopilación de los datos necesarios de un forma eficaz y eficiente para evaluar riesgos. Para obtener más información sobre la evaluación, consulte "Evaluaciones" en la página 189.

Mejoras en el Creador de cuestionarios - árbol de decisiones

Las respuestas a algunas preguntas llevan a preguntas adicionales. Al crear un cuestionario, ahora se puede expresar esta relación creando una relación condicional entre preguntas y mostrándolas en forma de un árbol de decisiones.

Mejoras en el panel de instrumentos del Centro de control y mandatos de seguridad

Panel de instrumentos del Centro de control y mandatos de seguridad mejorado con más visualizaciones y una mayor facilidad de uso que ayuda a comprender e interpretar fácilmente la información. Para obtener más información sobre el panel de control, consulte "Panel de control del Centro de control y mandatos de seguridad" en la página 139

Mejoras en el Panel de control de IBM Data Risk Manager

- Se cambia el widget Aplicación para mostrar los riesgos de datos y de privacidad de las aplicaciones asociadas a los activos de información.
- Se cambia la pantalla secundaria del panel de instrumentos para ver la información de riesgo de privacidad de OneTrust.

Mejoras en el modelador de datos

Mejoras en el componente modelador de datos con una nueva interfaz que facilita la creación de los diagramas.

Autenticación basada en Windows para el servidor MSSQL

Para el tipo de servidor MSSQL, si el servidor está habilitado para utilizar la autenticación de Windows, puede conectarse a la base de datos utilizando las credenciales de inicio de sesión de usuario de Windows para la autenticación.

Autenticación LDAP

IBM Data Risk Manager se puede integrar con un servidor Lightweight Directory Access Protocol (LDAP) para importar los grupos de usuarios creados dicho servidor LDAP.

Novedades en IBM Data Risk Manager, versión 2.0.3

Descripción de las características y otra información específica de la versión 2.0.3 de IBM Data Risk Manager.

Business Context Modeling (BCM)

- Mejoras en la importación de datos de contexto de negocio para todos los orígenes de integración.
- Definición y suministro de programas, incluida la jerarquía BU de programas.
- Mejoras en la gestión de inventario que ahora incluye el servidor, la aplicación, la base de datos y el almacenamiento de archivos.
- Mejoras del modelador de datos con la nueva interfaz.
- Se permite actualizar la ubicación en el inventario.

Panel de control Activo de información

- Superposición de alertas de vulnerabilidad de IBM QRadar Security Intelligence Platform y de exploración de IBM Security AppScan Enterprise en los nodos de la infraestructura.
- Página de bienvenida con widgets configurables y función de zoom en widgets individuales.
- Splash – Mayor nivel de detalle para correlaciones específicas del país para residencia de datos, violaciones de políticas y vulnerabilidades.
- Splash - Violaciones y vulnerabilidades de políticas que pertenecen a la 10 principales infraestructuras.
- Integración de la vista Mapa de la infraestructura con el panel de control de IBM Data Risk Manager.
- Mejoras de riesgo de la infraestructura.
- Capacidad de configuración de widgets del panel de control – colores e iconos.
- Revelación de la pantalla secundaria del panel de control con capacidad avanzada para ver los delitos basados en la línea temporal y los incidentes de varios orígenes.
- Coloreado basado en categorías

Integración de IBM QRadar Security Intelligence Platform

- Alertas de proceso desde IBM QRadar Security Intelligence Platform
- Superposición de alertas de vulnerabilidad en la infraestructura (servidores).
- Activación de la exploración de evaluación de vulnerabilidades en puntos finales.
- Descarga de las vulnerabilidades de puntos finales en BCM.

Integración de IBM Security AppScan Enterprise

- Mejoras en el módulo de evaluación de vulnerabilidades y activación de exploraciones.
- Descarga de datos de IBM Security AppScan Enterprise en BCM.
- Superposición de alertas de vulnerabilidad en la aplicación.

Integración de ServiceNow

- Mejoras de datos de contexto para la activación de la importación de datos.
- Importación del contexto de negocio desde ServiceNow.
- Integración de la vista Mapa de la infraestructura con el panel de control de IBM Data Risk Manager.
- Soporte de autenticación basada en OAUTH para ServiceNow.

Integración de Imperva SecureSphere

Descarga de exploraciones de vulnerabilidad de Imperva SecureSphere.

Administración del servidor

- Se proporciona la pestaña Gestión central de la consola de administración para gestionar las actividades de reinicio del agente, actualizar la contraseña, distribuir el parche (HA), desbloquear el usuario y ver el estado del parche.
- Configuración de alta disponibilidad.
- Migración de la consola de administración a la suite de aplicaciones de IBM Data Risk Manager.

Gestión de identidad

- Integración de LDAP - importar grupos de usuarios.

Mejoras funcionales continuas

- Cambios funcionales en el módulo Taxonomía.
- Cambios funcionales en el panel de control de IBM Data Risk Manager - Página secundaria Activo de información.
- Cambios funcionales en la Supervisión de la actividad de base de datos de IBM Security Guardium.
- Mejoras del motor de riesgo.
- Mejoras en la pantalla de taxonomía con información de etiquetado de activos.
- Recuento de filas – bloqueo de tablas en la base de datos MSSQL.

Integración de IBM InfoSphere Information Governance Catalog

- Productize MVP2 de la versión actual.
- Importación y correlación de datos - Catálogo y contexto.
- Notificación continua (suscriptor Kafka).
- Descomponentización de IBM InfoSphere Information Governance Catalog.

Evaluación de controles

- Comercialización de MCP de evaluación de riesgos (incluidas mejoras).
- Mejora funcional identificada basada en comentarios MVP sobre usabilidad.
- Integración del centro de acción.
- Evaluación cualitativa de la clasificación/evaluación de activos.
- Soporte para varios modelos de puntuación (condición y acumulativo).
- Página de destino para evaluación de controles.
- Evaluación de infraestructura genérica
- Opción para cargar el archivo CSV para cuestionarios.

Novedades de IBM Data Risk Manager, Versión 2.0.2

Descripción de las nuevas características y otra información específica del release actual de IBM Data Risk Manager.

IBM Data Risk Manager, versión 2.0.2 proporciona las prestaciones siguientes:

Business Context Modeling (BCM)

- Mejoras en la importación de datos de contexto de negocio para todos los orígenes de integración.
- Definición y suministro de programas, incluida la jerarquía BU de programas.
- Mejoras en la gestión de inventario que ahora incluye el servidor, la aplicación, la base de datos y el almacenamiento de archivos.
- Mejoras del modelador de datos (simplificación de la interfaz de usuario).

Panel de control Activo de información

- Superposición de alertas de vulnerabilidad de IBM QRadar Security Intelligence Platform y de exploración de IBM Security AppScan Enterprise en los nodos de la infraestructura.
- Página de bienvenida con widgets configurables y función de zoom en widgets individuales.
- Integración de la vista Mapa de la infraestructura con el panel de control de IBM Data Risk Manager.
- Adiciones de riesgos de infraestructura.

Integración de IBM QRadar Security Intelligence Platform

- Alertas de proceso desde IBM QRadar Security Intelligence Platform
- Superposición de alertas de vulnerabilidad en la infraestructura (servidores).
- Activación de la exploración de evaluación de vulnerabilidades en puntos finales.
- Descarga de las vulnerabilidades de puntos finales en BCM.

Integración de IBM Security AppScan Enterprise

- Mejoras en el módulo de evaluación de vulnerabilidades y activación de exploraciones.
- Descarga de datos de IBM Security AppScan Enterprise en BCM.
- Superposición de alertas de vulnerabilidad en la aplicación.

Integración de ServiceNow

- Mejoras de datos de contexto para la activación de la importación de datos.
- Importación del contexto de negocio desde ServiceNow.
- Integración de la vista Mapa de la infraestructura con el panel de control de IBM Data Risk Manager.

Administración del servidor

- Se proporciona la pestaña Gestión central de la consola de administración para gestionar las actividades de reinicio del agente, actualizar la contraseña, distribuir el parche (HA), desbloquear el usuario y ver el estado del parche.
- Configuración de alta disponibilidad.

Gestión de identidad

- Integración de LDAP - importar grupos de usuarios.

Mejoras funcionales continuas

- Cambios funcionales en el módulo Taxonomía.

- Cambios funcionales en el panel de control de IBM Data Risk Manager - Página secundaria Activo de información.
- Cambios funcionales en la Supervisión de la actividad de base de datos de IBM Security Guardium.
- Mejoras del motor de riesgo.

Integración de IGC

- Productize MVP2 de la versión actual.
- Importación y correlación de datos - Catálogo y contexto.
- Notificación continua (suscriptor Kafka).

Imágenes de instalación y fixpacks

Obtenga los archivos de instalación de IBM Data Risk Manager desde el sitio web de IBM® Passport Advantage y los fixpacks de Fix Central.

El sitio web de Passport Advantage proporciona paquetes, a los que se hace referencia como eAssemblies, para varios productos de IBM en http://www-01.ibm.com/software/passportadvantage/pao_customer.html.

Puede utilizar Fix Central para buscar los arreglos proporcionados por el servicio de soporte de IBM para una variedad de productos, incluido IBM Data Risk Manager en https://www-945.ibm.com/support/fixcentral. Con Fix Central, puede buscar, seleccionar, solicitar y descargar arreglos para su sistema con una amplia gama de opciones de entrega.

Instalación y configuración

La instalación es una actividad mediante la que se coloca software en sistemas.

Los temas de instalación proporcionan información sobre el software y el hardware de requisito previo y también la instalación del producto.

Los temas de configuración se centran en la configuración inicial y en la personalización del producto.

Visión general de la instalación

Instale IBM Data Risk Manager en un entorno virtual utilizando la plataforma VMware. IBM Data Risk Manager se proporciona como una aplicación virtual de VMware en formato OVA (Open Virtual Appliance).

IBM Data Risk Manager se despliega como una solución local, desarrollada como una aplicación web basada en el modelo de arquitectura de cliente/servidor. Puede configurar la aplicación para admitir distintos requisitos no funcionales como, por ejemplo, gestión de alta disponibilidad y recuperación tras desastre.

Requisitos previos de instalación

Antes de instalar y desplegar IBM Data Risk Manager, conozca los requisitos previos y planee su entorno.

Especificaciones de hardware para una máquina virtual (VM) de servidor autónomo

Procesador	5 GHz o superior
Número de procesadores	4
Memoria (RAM)	16 GB
Red	Dual de 1 Gbps

Almacenamiento	200 GB
Arquitectura	de 64 bits

Especificaciones de software para desplegar la imagen virtual de IBM Data Risk Manager (archivo OVA)

Sistema operativo	Host de máquina virtual: VMware ESXi 5.5 o posterior
Conectividad	LAN de 100 Mbps
Despliegue y mantenimiento	El servidor puede ser accesible a través de la intranet (mediante una VPN) para la instalación y configuración.

Especificaciones de cliente para escritorios, cuadernos o estaciones de trabajo

CPU	2,33 GHz (compatible con x86)
Memoria (RAM)	4 GB
Sistema operativo	Microsoft Windows 10 / Mac OSX
Navegador	Chrome 59 o posterior y Firefox 52 o posterior

Bases de datos admitidas

Base de datos	**Versión**
MySQL	5.7.19+
Oracle	11g y 12c
SQL Server	Server 2012 y Server 2016
Sybase	16.0
IBM Db2	11.1
Postgres	9.6+

Aceleradores de integración

IBM Data Risk Manager se puede integrar con los productos siguientes que ofrecen un proceso programático para el descubrimiento continuo, la clasificación y la creación de informes de datos confidenciales, así como los riesgos asociados en toda la empresa.

Producto	**Versión**
IBM Security Guardium	10.5.0, 10.6.0 y 11.0
IBM Security AppScan Enterprise	9.0.3.8
DLP de Symantec	12.x y 14.x
IBM QRadar Security Intelligence Platform	7.3.1
IBM InfoSphere Information Governance Catalog	11.5 y 11.7
Imperva SecureSphere	13.0.0.10
ServiceNow	Kingston
OneTrust	NA

Producto	Versión
IBM Multi-Cloud Data Encryption	2.2
IBM Security Guardium Analyzer	NA
IBM StoredIQ	7.6.0.17

Valores de configuración de red

Protocolo/ puerto	Servicio	Origen	Destino
22/TCP	**ssh** Acceso a la línea de mandatos para administrar y gestionar el servidor de IBM Data Risk Manager.	Escritorio remoto	Servidor de IBM Data Risk Manager
9003/TCP	**Syslog** Recibe notificaciones de syslog desde el dispositivo IBM Security Guardium.	Dispositivo IBM Security Guardium (si está instalado)	Servidor de IBM Data Risk Manager
9000/TCP	**Syslog** Recibe notificaciones de syslog desde el dispositivo IBM QRadar Security Intelligence Platform.	Dispositivo IBM QRadar Security Intelligence Platform (si está instalado)	Servidor de IBM Data Risk Manager
8009 /TCP	**AJP** Para alta disponibilidad (HA) de IBM Data Risk Manager.	Servidor HA de IBM Data Risk Manager	Servidor de IBM Data Risk Manager
8443/TCP	**https** Conectividad del servidor de IBM Data Risk Manager con las aplicaciones cliente de IBM Data Risk Manager.	Comunicación bidireccional entre las aplicaciones cliente de IBM Data Risk Manager y el servidor de IBM Data Risk Manager	Navegadores web soportados
8762/TCP	Escáner de base de datos nativa	Servidor de IBM Data Risk Manager	Sistemas de destino donde están alojados los servidores de bases de datos. Por ejemplo, Oracle, MySQL o SQL Server.
8764/TCP	Agente DLP de Symantec	Servidor de IBM Data Risk Manager	Dispositivo DLP de Symantec
8765/TCP	Agente de identidad de seguridad	Comunicación bidireccional entre el agente de identidad de seguridad y el servidor LDAP/SSO	El puerto del servidor LDAP tiene que estar abierto en 389 (LDAP) o en 636 (servidor de LDAP y SSO)

Protocolo/ puerto	Servicio	Origen	Destino
8766/TCP	Escáner no estructurado	Servidor de IBM Data Risk Manager	Sistema de compartición de archivos remoto de destino donde están habilitados SMB o SFTP.
8768/TCP	Escáner de IBM InfoSphere Information Governance Catalog	Servidor de IBM Data Risk Manager	Dispositivo IBM InfoSphere Information Governance Catalog
8787/TCP	Agente ServiceNow	Servidor de IBM Data Risk Manager	Dispositivo ServiceNow
2529/TCP	Agente de gestión de IBM Data Risk Manager	Servidor de IBM Data Risk Manager	Servidor de IBM Data Risk Manager

Lista de comprobación del despliegue

- Elija la ubicación en la que colocar la máquina virtual del servidor de IBM Data Risk Manager.
- Documente la dirección IP y el nombre de host para asignar a la máquina virtual del servidor de IBM Data Risk Manager.
- Asegúrese de que el servidor de IBM Data Risk Manager y los servidores de base de datos están conectados.
- Determine los productos y las aplicaciones que se van a integrar con IBM Data Risk Manager y asegúrese de que están disponibles y son accesibles.
- Creación de una cuenta de servicio en los productos de integración y las bases de datos que están en el ámbito con los privilegios necesarios para ejecutar exploraciones de metadatos.

Implementación de la imagen virtual de IBM Data Risk Manager

Para instalar IBM Data Risk Manager en un entorno de VMware, implemente la plantilla OVA del dispositivo. La implementación de una plantilla OVA crea un dispositivo virtual que contiene la aplicación en un host VMware como, por ejemplo, un servidor ESXi.

Antes de empezar

- Descargue y extraiga el paquete OVA de IBM Data Risk Manager a un directorio. El archivo está disponible para su descarga desde el sitio web de IBM Passport Advantage. Consulte el tema “Instrucciones de descarga de software ” en la página 3 para obtener detalles.
- Revise el tema Requisitos previos de instalación para conocer la información de requisito previo para la instalación y configuración de IBM Data Risk Manager.

Procedimiento

1. Descargue el archivo de instalación de la plantilla de OVA de IBM Data Risk Manager desde Passport Advantage Online.
2. Abra el cliente de VMware vSphere.
3. Seleccione **File (Archivo)** > **Deploy OVF Template (Implementar plantilla de OVF)**.
4. Pulse **Examinar** para localizar el archivo OVA que ha descargado y seleccionar el archivo.
5. Pulse **Siguiente**.
6. Proporcione un nombre significativo para la plantilla, que se convertirá en el nombre de la máquina virtual. Identifique una ubicación adecuada para desplegar la máquina virtual. Pulse **Siguiente**.
7. Seleccione **Thick Provision Lazy Zeroed (Aprovisionamiento completo con puesta a cero diferida)** como el formato de disco para almacenar los discos virtuales. Se recomienda seleccionar thick

provisioning (aprovisionamiento completo), que está preseleccionado para obtener un rendimiento optimizado. Pulse **Siguiente**.

8. Correlacione las redes para la plantilla desplegada que va a utilizar. Pulse **Destination Networks (Redes de destino)** para ver las redes disponibles en el servidor ESX. Seleccione una red de destino para definir la asignación de dirección IP adecuada para el despliegue de la máquina virtual. Pulse **Siguiente**.
9. Revise los valores de despliegue. Si desea que el servidor se inicie tan pronto como se despliegue, seleccione **Power on after deployment (Encender después de la implementación)**.
10. Pulse **Finalizar** para cerrar el asistente para implementar plantillas de OVF e implementar la máquina virtual. La implementación de la máquina virtual puede tardar varios minutos.

Qué hacer a continuación

Defina la configuración de IBM Data Risk Manager utilizando la interfaz de línea de mandatos del servidor de IBM Data Risk Manager. Para obtener más información, consulte Configuración del servidor de IBM Data Risk Manager.

Utilice el cliente de VMware vSphere para configurar las opciones de hardware de dispositivo virtual para el dispositivo virtual de IBM Data Risk Manager. Para obtener más información, consulte Actualización del disco duro y Actualización de la RAM.

Configuración del servidor de IBM Data Risk Manager

Después de que se despliegue el dispositivo virtual de IBM Data Risk Manager en el entorno de VMware, debe completar algunas tareas de configuración.

Antes de empezar

Asegúrese de que la imagen virtual de IBM Data Risk Manager se ha desplegado correctamente en un entorno de VMware. Para obtener información sobre cómo desplegar la imagen virtual, consulte “Implementación de la imagen virtual de IBM Data Risk Manager” en la página 21.

Acerca de esta tarea

Después de que se despliega en dispositivo IBM Data Risk Manager en una red virtual, debe completar la configuración inicial utilizando la interfaz de línea de mandatos del servidor.

Procedimiento

1. Inicie sesión en la máquina virtual de IBM Data Risk Manager utilizando el nombre de usuario y la contraseña predeterminados.

   ```
   idrm-server: a3user
   Password: idrm
   ```

   Tras el primer inicio de sesión, a3user puede ejecutar el mandato **passwd** para cambiar la contraseña predeterminada.
2. Asigne la dirección IP al servidor.

   IBM Data Risk Manager

   a. Ejecute el mandato siguiente para ver las interfaces de red activas (Ethernet) en la máquina virtual, que está en el formato `ifcfg-XX`.

      ```
      # ip a
      ```

      Salida de ejemplo del mandato `ip a`

      ```
      [a3user@idrm-server ~]$ ip a
      1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
          link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
          inet 127.0.0.1/8 scope host lo
      ```

```
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:0f:47:46 brd ff:ff:ff:ff:ff:ff
```

En este ejemplo, ens33 representa el valor de XX en el formato ifcfg-XX.

b. En la salida del mandato, el valor de XX en el formato ifcfg-XX es distinto de ens33, por ejemplo, ens66 o eth0, ejecute el paso siguiente.

Vaya al directorio siguiente y compruebe si existe el archivo ifcfg-XX.

```
cd /etc/sysconfig/network-scripts
```

Si existe el archivo ifcfg-XX, vaya al paso c. De lo contrario, ejecute el mandato siguiente.

```
# sudo mv /etc/sysconfig/network-scripts/ifcfg-33 /etc/sysconfig/network-scripts/ifcfg-XX
# sudo rm -f /etc/sysconfig/network-scripts/ifcfg-33
```

c. Ejecute el mandato siguiente para localizar y abrir el archivo de configuración de interfaz para editarlo.

```
# # sudo vi /etc/sysconfig/network-scripts/ifcfg-XX
```

d. Edite las siguientes propiedades en el archivo de configuración de interfaz. Mantenga los valores predeterminados para las propiedades restantes.

BOOTPROTO	dhcp o static
NAME	XX, por ejemplo ens33
DEVICE	XX, por ejemplo ens33
IPADDR	Dirección IP asignada a IBM Data Risk Manager, por ejemplo, 9.195.17.227.
PREFIX	Máscara de subred, por ejemplo, 23.
NETMASK	Dirección de máscara de subred de red predeterminada, por ejemplo, 255.255.254.0.
GATEWAY	Dirección IP de pasarela de red predeterminada, por ejemplo 9.195.16.1.
DNS1	Dirección del servidor de nombres de dominio (DNS), por ejemplo, 9.0.146.50.
DNS2	Dirección DNS, por ejemplo, 9.0.148.50.

El ejemplo siguiente muestra el contenido del archivo.

```
[a3user@idrm-server network-scripts]$ cat ifcfg-ens33
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="static"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="ens33"
UUID="0e46ed9e-4144-403a-9b20-4235da5199ac"
DEVICE="ens33"
ONBOOT="yes"
IPADDR="9.195.20.86"
PREFIX=0
NETMASK="255.255.255.0"
GATEWAY="9.195.20.1"
```

```
DNS1="9.0.146.50"
DNS2="9.0.148.50"
```

e. (Opcional) Configure el servidor DNS.

```
# sudo vi /etc/resolv.conf
name server <su_ip_servidor>
```

f. Reinicie el servicio de red.

```
# sudo service network restart
```

g. En el caso del formato VHD, hay que jecutar el siguiente comando:

```
sudo ifdown etho
        sudo ifup eth0
```

h. Para obtener la dirección IP real en los formatos OVA y VHD, ejecute el siguiente comando:

```
ip a
```

3. Asigne el nombre de host o añada `datariskmanager-server.ibm.com` en la lista de DHCP de red.

```
# sudo sysctl kernel.hostname=<nombre_host>
      # sudo service network restart
      # sudo vi /etc/sysconfig/network
      HOSTNAME=<nombre_host>
      # sudo reboot
```

4. Asigne la fecha, la hora y el huso horario al servidor de IBM Data Risk Manager.

a. Establezca la fecha y la hora para el servidor de IBM Data Risk Manager.

```
# sudo service ntpd stop
      # sudo ntpdate -q <nombre_dns_servidor_ntp_o_dirección_ip>
      # sudo service ntpd start
```

Asegúrese de que la zona horaria del servidor NTP sea correcta.

b. Ejecute el mandato siguiente para verificar la fecha y la hora.

```
# date
```

c. Ejecute el mandato siguiente para asegurarse de que el reloj de hardware esté sincronizado con la fecha y hora del sistema.

```
sudo hwclock --systohc
```

d. Ejecute el mandato siguiente para verificar si se actualiza la fecha y hora del reloj de hardware.

```
sudo hwclock
```

e. Actualice el huso horario.

1)
```
# sudo mv /etc/localtime /root/localtime.old
      # sudo ln -s /usr/share/zoneinfo/<zona>/<Location> /etc/localtime
```

2) Ejecute el mandato siguiente para verificar si el huso horario se ha actualizado correctamente.

```
 # date
```

f. Si se actualiza el huso horario, suprima el archivo antiguo y reinicie el servidor.

```
# sudo rm -f /root/localtime.old
      # reboot
```

Qué hacer a continuación

Verifique si puede acceder a la suite de aplicaciones de IBM Data Risk Manager.

1. Abra la suite de aplicaciones de IBM Data Risk Manager utilizando el URL siguiente.

```
https://<dirección-IP-servidor-IDRIM>:8443/albatross/a3suite
```

2. Especifique el nombre de usuario y la contraseña siguientes.

```
User name: admin
Password: a3!BM!DNA
```

3. Cambie la contraseña cuando se le solicite.
4. Acepte el acuerdo de licencia.
5. Registre la dirección IP en la Consola de administración de IBM Data Risk Manager.
   a. Inicie sesión en la consola de administración de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/index`) como usuario `admin`.
   b. Pulse **Gestión central**.
   c. Pulse **Registrar**.
   d. Especifique la dirección IP en **Dirección IP de host**.
   e. Si la contraseña SSH de `a3user` se modifica, especifique la contraseña SSH en **Contraseña SSH de host**.
   f. Pulse **Registrar**.
   g. Pulse **Actualizar contraseña**.
   h. Especifique la contraseña actualizada en **Actualizar contraseña**.
   i. Pulse **Actualizar**.

Aumento de la memoria virtual

Es posible que tenga que aumentar la memoria virtual para obtener un mejor rendimiento de IBM Data Risk Manager.

Antes de empezar

La máquina virtual que está configurando debe estar apagada.

Acerca de esta tarea

Aumente el tamaño de memoria de 16 GB a 32 GB en la máquina virtual.

Procedimiento

1. Pulse **Máquina virtual** > **Valores**.
2. En la sección Memoria, establezca la cantidad de memoria que se debe asignar a la máquina virtual utilizando el control deslizante **Memoria**.
3. Guarde los valores.
4. Inicie la máquina virtual.

Qué hacer a continuación

Verifique los valores de memoria.

1. Inicie sesión en el dispositivo virtual de IBM Data Risk Manager utilizando el nombre de usuario y la contraseña predeterminados.
2. En la interfaz de línea de mandatos, ejecute el mandato siguiente para visualizar el tamaño de la memoria en GB.

```
free -g
```

Aumento del tamaño del disco duro virtual

Si el espacio de disco preconfigurado no es suficiente, puede aumentar el tamaño del disco virtual para IBM Data Risk Manager.

Antes de empezar

La máquina virtual que está configurando debe estar apagada.

Acerca de esta tarea

Aumente el tamaño del disco duro de 200 GB a 300 GB en la máquina virtual. Después de que aumente el tamaño del disco virtual, tiene que aumentar la partición de disco duro. Se puede utilizar la herramienta de particionamiento `GParted` para el particionamiento.

Procedimiento

1. Pulse **Máquina virtual** > **Valores**.
2. Seleccione el disco de máquina virtual de IBM Data Risk Manager, por ejemplo, `idna-server-disk.vmdk`.
3. Utilice el graduador **Tamaño de disco** para establecer el nuevo tamaño.
4. Para cambiar el tamaño del disco duro virtual, pulse **Aplicar**.
5. Pulse **Aceptar**.
6. Conecte el CD.
7. Asigne la unidad de CD al archivo ISO `GParted`.
8. Seleccione la opción **CD/DVD** para iniciar la máquina virtual. Pulse **Reiniciar** para iniciar la herramienta de particionamiento GParted.
9. Para un teclado predeterminado, seleccione la opción **No cambiar teclado**.
10. Seleccione el idioma especificando el número que corresponda al idioma preferido y pulse Intro. El valor predeterminado es inglés de EE.UU.
11. Seleccione el modo de visualización escribiendo el número de su modo preferido y pulse Intro.

    Se mostrará la página "**/dev/sda - GParted**".
12. Pulse **Partición** > **Redimensionar/mover**.
13. En la página "**Redimensionar/mover /dev/sda1**", especifique los valores siguientes.

Opción	Descripción
Espacio libre anterior (MiB)	0
Tamaño nuevo (MiB)	255999
Espacio libre siguiente (MiB)	0
Alinear a	MiB

14. Pulse **Redimensionar/mover**.
15. Pulse **Aplicar**.
16. Pulse **Cerrar** cuando la acción se complete correctamente.
17. Pulse **Salir**.
18. Para reiniciar la máquina virtual, seleccione **Rearrancar**.

Qué hacer a continuación

Verifique el tamaño del disco duro.

1. Inicie sesión en el dispositivo virtual de IBM Data Risk Manager utilizando el nombre de usuario y la contraseña predeterminados.

2. En la interfaz de línea de mandatos, ejecute el mandato siguiente para visualizar el tamaño del disco duro.

```
df -h
```

Configuración de alta disponibilidad en IBM Data Risk Manager

Para ayudar a mantener las operaciones continuas de IBM Data Risk Manager, puede configurar el entorno para obtener una alta disponibilidad.

Configuración de alta disponibilidad

La habilitación de la función de alta disponibilidad de IBM Data Risk Manager en un entorno de infraestructura integrado minimiza el tiempo de inactividad del sistema y proporciona la capacidad de recuperación tras desastre.

Terminologías utilizadas en la configuración de alta disponibilidad

Nodo primario
El cliente utiliza la instancia de máquina virtual de nodo primario para acceder a IBM Data Risk Manager. Se ejecuta el servidor de equilibrio de carga de IBM Data Risk Manager y la base de datos maestra en el nodo primario.

Nodo BD
La base de datos esclava de IBM Data Risk Manager se ejecuta en la instancia de máquina virtual de nodo BD.

Nodo de aplicación
Los servicios que son necesarios para ejecutar IBM Data Risk Manager deben estar en ejecución en todas las instancias de máquina virtual del nodo de aplicación.

Base de datos maestra
La base de datos de la instancia de máquina virtual de nodo primario es la base de datos maestra. Las operaciones de lectura y escritura se pueden realizar en la base de datos maestra.

Base de datos esclava
La base de datos de la instancia de máquina virtual del nodo de máquina virtual es la base de datos esclava. Solo se puede realizar la operación de escritura en la base de datos esclava.

Requisitos y consideraciones para la configuración de alta disponibilidad

- En la actualidad, para la alta disponibilidad de IBM Data Risk Manager, puede configurar un nodo primario, un nodo BD y un máximo de dos nodos de aplicación.
- El nodo primario debe estar siempre en ejecución para acceder al nodo de aplicación.
- Si uno de los nodos de aplicación de IBM Data Risk Manager está inactivo, el otro nodo de aplicación puede continuar al servicio de las solicitudes.
- Si el nodo BD de IBM Data Risk Manager está inactivo, puede continuar utilizando el sistema IBM Data Risk Manager. Cuando el nodo BD está activo y en ejecución, los datos delta capturados se duplican automáticamente en el nodo BD (esclava).
- Asegúrese de que los nodos de aplicación deben tener un mínimo de 16 GB de RAM.
- Durante el proceso de configuración, puede salir en cualquier momento si fuera necesario. Sin embargo, una vez completado el proceso de configuración en una instancia de máquina virtual de IBM Data Risk Manager, no se puede revertir. Debe volver a instalar la instancia de máquina virtual y volver a iniciar el proceso de configuración.
- Si una instancia de máquina virtual de IBM Data Risk Manager ya está configurada como nodo primario, nodo BD o nodo de aplicación, no se permite la configuración adicional.

Proceso de configuración de alta disponibilidad

Para configurar un entorno de alta disponibilidad en IBM Data Risk Manager, complete los pasos siguientes.

1. Instale, por ejemplo, IBM Data Risk Manager en cuatro instancias de máquina virtual. Para ver los pasos de instalación, consulte “Implementación de la imagen virtual de IBM Data Risk Manager” en la página 21.
2. Determine cuál de las máquinas virtuales actúan como nodo primario, nodo BD o nodo de aplicación.
3. Configure la máquina virtual del nodo primario. Consulte “Configuración del nodo primario” en la página 30 para obtener información sobre los pasos de configuración.
4. Configure la máquina virtual del nodo BD. Consulte “Configuración del nodo de base de datos” en la página 30 para obtener información sobre los pasos de configuración.
5. Configure las máquinas virtuales del nodo de aplicación. Consulte “Configuración de nodos de aplicación” en la página 31 para obtener información sobre los pasos de configuración.
6. Después de la configuración de todas las instancias de máquina virtual para alta disponibilidad, puede acceder a IBM Data Risk Manager utilizando la dirección web siguiente:

   ```
   https://DIRECCIÓN_IP_NODO_PRIMARIO:8443/albatross/A3Suite
   ```

7. Puede ver el estado de la alta disponibilidad de IBM Data Risk Manager en la ubicación siguiente.

   ```
   https://DIRECCIÓN_IP_NODO_PRIMARIO:80/status
   ```

Resolución de problemas de configuración de alta disponibilidad y método alternativo

Los archivos de registro se generan cuando las instancias de máquina virtual de IBM Data Risk Manager están configuradas para la alta disponibilidad que el equipo de soporte puede utilizar para resolver problemas. Los archivos de registro se almacenan en `~/agile3/HA_Configure.log`.

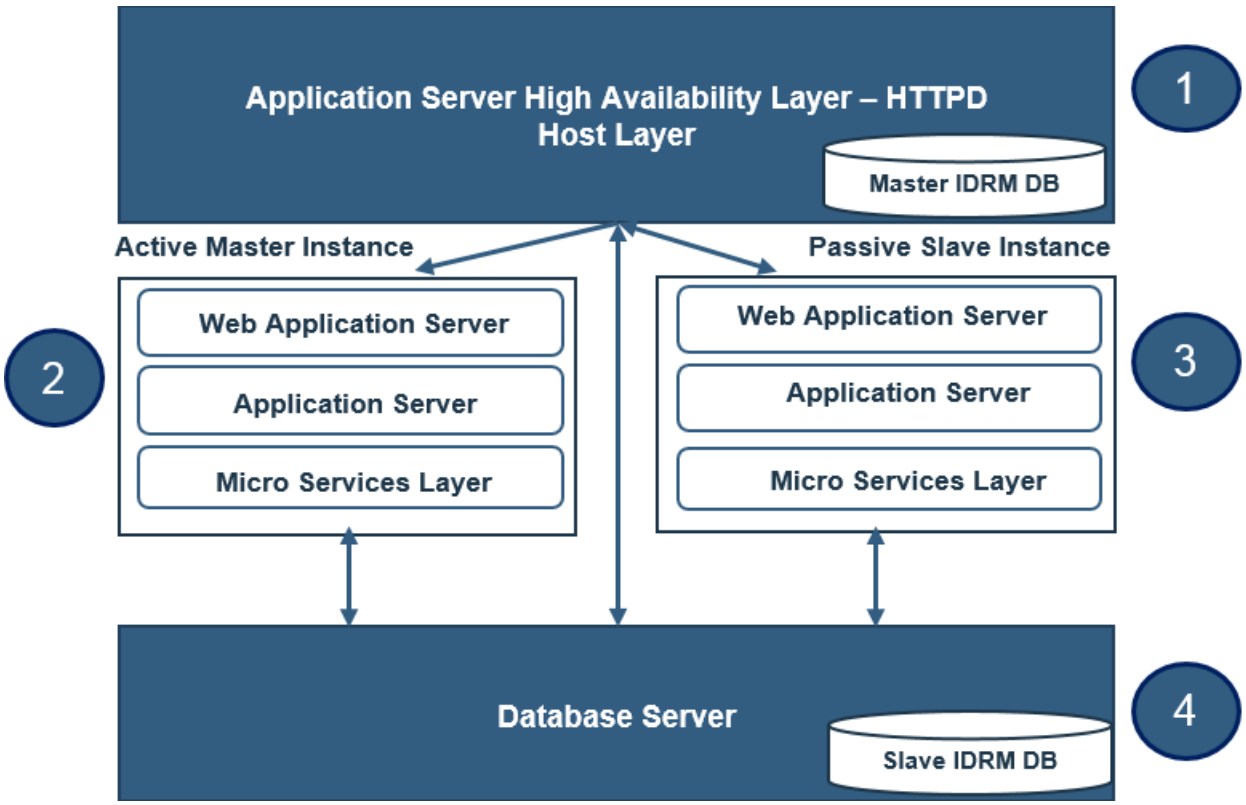
Para obtener más información acerca de cómo resolver problemas de configuración de alta disponibilidad, consulte “Problemas de configuración de alta disponibilidad y método alternativo” en la página 234.

Modelo de despliegue de alta disponibilidad de IBM Data Risk Manager

IBM Data Risk Manager admite arquitectura de despliegue de cuatro hosts para alta disponibilidad.

Modelo de despliegue de alta disponibilidad de IBM Data Risk Manager

El diagrama siguiente muestra el modelo de despliegue de alta disponibilidad de IBM Data Risk Manager. La réplica de primario y en espera utiliza la sincronización y la fiabilidad de WAL (Write-Ahead Log, registro de grabación anticipada).



Requisitos de sistema host para el despliegue de alta disponibilidad

	Host 1	**Host 2**	**Host 3**	**Host 4**
Componentes	Capa de alta disponibilidad del servidor de aplicaciones y base de datos maestra	Servidor de aplicaciones de IBM Data Risk Manager (maestro)	Servidor de aplicaciones de IBM Data Risk Manager (esclavo)	Servidor de base de datos (esclavo)
Procesador	Intel Quad-core XEON a 2 GHz o superior	Intel Quad-core XEON a 2 GHz o superior	Intel Quad-core XEON a 2 GHz o superior	Intel Quad-core XEON a 2 GHz o superior
Número de procesadores	4	4	4	4
Memoria (RAM)	16 GB	16 GB	16 GB	16 GB
Red	Dual de 1 Gbps	Dual de 1 Gbps	Dual de 1 Gbps	Dual de 1 Gbps
Almacenamiento	200	200	200	200
Sistema operativo	Host de máquina virtual: VMWare ESXi 5.5 y superior	Host de máquina virtual: VMWare ESXi 5.5 y superior	Host de máquina virtual: VMWare ESXi 5.5 y superior	Host de máquina virtual: VMWare ESXi 5.5 y superior
Arquitectura	SO/JVM de 64 bits	SO/JVM de 64 bits	SO/JVM de 64 bits	SO/JVM de 64 bits
Conectividad	Admite internet e intranet	Admite internet e intranet	Admite internet e intranet	Admite internet e intranet

Despliegue y mantenimiento	El servidor debe ser accesible a través de la intranet (mediante una VPN) para la instalación y configuración.	El servidor debe ser accesible a través de la intranet (mediante una VPN) para la instalación y configuración.	El servidor debe ser accesible a través de la intranet (mediante una VPN) para la instalación y configuración.	El servidor debe ser accesible a través de la intranet (mediante una VPN) para la instalación y configuración.

Configuración del nodo primario

Debe configurar el nodo primario para configurar la alta disponibilidad de IBM Data Risk Manager. El clúster de alta disponibilidad de IBM Data Risk Manager está formado por un nodo primario donde se ejecutan el servidor de equilibrio de carga y la base de datos maestra.

Antes de empezar

Asegúrese de que la contraseña de a3user está disponible.

Antes de configurar el nodo primario, revise las consideraciones y las restricciones que se listan en el tema "Configuración de alta disponibilidad" en la página 27.

Procedimiento

1. Inicie sesión en la instancia de máquina virtual (VM) de IBM Data Risk Manager que se debe configurar como nodo primario, como a3user, sobre SSH.
2. Vaya al siguiente directorio.

   ```
   cd IDRM_HA_Config/
   ```

3. Desde la línea de mandatos, ejecute el script siguiente.

   ```
   ./configure_ha
   ```

4. Especifique el número de nodos de aplicación que desea configurar. Se puede configurar un máximo de dos nodos.
5. Especifique el número de nodo de base de datos que se debe configurar. Solo se puede configurar un nodo de base de datos.
6. Especifique la dirección IP de los nodos de aplicación.
7. Especifique la dirección IP del nodo de base de datos.

   La operación de configuración se inicia solo cuando las direcciones IP especificadas son correctas. Una vez finalizado el proceso de configuración, se visualiza un mensaje de alerta para configurar el nodo BD y el nodo de aplicación antes de utilizar IBM Data Risk Manager.

Qué hacer a continuación

Configure el nodo BD. Consulte "Configuración del nodo de base de datos" en la página 30 para obtener información sobre los pasos de configuración.

Configuración del nodo de base de datos

Debe configurar el nodo de base de datos para configurar la alta disponibilidad de IBM Data Risk Manager. El clúster de alta disponibilidad de IBM Data Risk Manager está formado por un nodo de base de datos donde se ejecuta la base de datos esclava.

Antes de empezar

Asegúrese de que la contraseña de a3user está disponible.

Antes de configurar el nodo de base de datos, revise las consideraciones y las restricciones que se listan en el tema "Configuración de alta disponibilidad" en la página 27.

Procedimiento

1. Inicie sesión en la instancia de máquina virtual (VM) de IBM Data Risk Manager que se debe configurar como un nodo de base de datos, como a3user a través de SSH.
2. Vaya al siguiente directorio.

   ```
   cd IDRM_HA_Config/
   ```

3. Desde la línea de mandatos, ejecute el script siguiente.

   ```
   ./configure_ha
   ```

4. Especifique el número de nodos de aplicación que desea configurar. Se puede configurar un máximo de dos nodos. Debe especificar el mismo número que ha especificado durante la configuración del nodo primario.
5. Especifique el número de nodo primario que se debe configurar. Solo se puede configurar un nodo primario.
6. Especifique la dirección IP de los nodos de aplicación.
7. Especifique la dirección IP del nodo primario.

   La operación de configuración se inicia solo cuando las direcciones IP especificadas son correctas. Una vez completado el proceso de configuración, se visualiza un mensaje de alerta para indicar que el nodo de base de datos (base de datos esclava) está enlazado con el nodo primario (Base de datos maestra).

Qué hacer a continuación

Configure el nodo de aplicación. Consulte “Configuración de nodos de aplicación” en la página 31 para obtener información sobre los pasos de configuración.

Configuración de nodos de aplicación

Debe configurar el nodo de aplicación para configurar la alta disponibilidad de IBM Data Risk Manager. El clúster de alta disponibilidad de IBM Data Risk Manager puede contener un máximo de dos nodos de aplicación.

Antes de empezar

Asegúrese de que la contraseña de a3user está disponible.

Antes de configurar el nodo de aplicación, revise las consideraciones y las restricciones que se listan en el tema “Configuración de alta disponibilidad” en la página 27.

Procedimiento

1. Inicie sesión en la instancia de máquina virtual (VM) de IBM Data Risk Manager que se debe configurar como un nodo de aplicación, como a3user a través de SSH.
2. Vaya al siguiente directorio.

   ```
   cd IDRM_HA_Config/
   ```

3. Desde la línea de mandatos, ejecute el script siguiente.

   ```
   ./configure_ha
   ```

4. Especifique el número de nodo primario que se debe configurar. Solo se puede configurar un nodo primario.
5. Especifique la dirección IP del nodo primario.

   La operación de configuración se inicia solo cuando la dirección IP especificada es correcta. Una vez finalizado el proceso de configuración, se visualiza un mensaje para indicar que el nodo de aplicación está enlazado con el nodo primario (sistema de equilibrador de carga).

Qué hacer a continuación

Después de la configuración de todas las instancias de máquina virtual para alta disponibilidad, puede acceder a IBM Data Risk Manager utilizando la dirección web siguiente:

```
https://DIRECCIÓN_IP_NODO_PRIMARIO:8443/albatross/A3Suite
```

Puede ver el estado de la alta disponibilidad de IBM Data Risk Manager en la ubicación siguiente.

```
https://DIRECCIÓN_IP_NODO_PRIMARIO:80/status
```

Administración de IBM Data Risk Manager

Los temas de administración explican la configuración y los valores de servidor necesarios para realizar funciones de IBM Data Risk Manager sin problemas.

Las actividades de administración incluyen las siguientes tareas:

- Valores de servidor
- Suministro de usuarios
- Configuraciones de adaptador
- Otras tareas administrativas

Antes de empezar, familiarícese con los conceptos y la terminología que se mencionan en esta sección. Consulte las secciones Visión general del producto e Instalación y configuración para obtener la información relacionada.

IBM Data Risk Manager Administration

Utilice el componente IBM Data Risk Manager Administration para ejecutar las tareas administrativas para instalar y configurar los distintos aspectos del entorno de IBM Data Risk Manager. Solo los usuarios con el rol `Superadministrador` pueden realizar operaciones administrativas.

Acceso al componente IBM Data Risk Manager Administration

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Pulse **Administración**.

En las secciones siguientes se describen varias opciones de la página **Administración** para ejecutar las tareas administrativas.

Diagnóstico

Pulse **Diagnóstico** para ver el estado de los microservicios de IBM Data Risk Manager, ver los detalles de registro de microservicio, configurar los niveles de registro y reiniciar las instancias de microservicio.

`Full Stack` es la instancia de IBM Data Risk Manager principal y no se puede modificar. Para reiniciar una instancia de microservicio, pulse **Reiniciar**.

Pulse la pestaña **Registros** para ver y descargar los archivos de registro para una instancia de microservicio. Los archivos de registro están categorizados en cuatro niveles diferentes.

Depuración
En este nivel, se registran todos los mensajes de varias instancias de microservicio.

Interacción
En este nivel, se registran todos los mensajes que se generan entre el servidor y los microservicios.

Operativo
En este nivel, se registran todas las operaciones en todos los microservicios.

Aviso
En este nivel, se registran todas las excepciones en todos los microservicios. Este es el valor predeterminado y se sugiere para el entorno de producción.

Puede utilizar la sección **Habilitar niveles de registro** para establecer dinámicamente los niveles de registro.

Gestionar transacciones de carga

Pulse **Gestionar transacciones de carga** para ver los detalles de la exploración, los detalles del usuario que ha iniciado el proceso de exploración y la fecha y la hora en que se ha iniciado el proceso de exploración.

Registros de auditoría

Pulse **Registros de auditoría** para ver los detalles del archivo de registro de auditoría. El archivo contiene detalles relacionados con varios usuarios de IBM Data Risk Manager. Puede buscar sucesos específicos de registros de auditoría basándose en el nombre de usuario, el tipo de solicitud o el tipo de actividad.

Configuración del servidor

Una vez que se ha completado el proceso de instalación de IBM Data Risk Manager, debe realizar las configuraciones iniciales antes de que sea funcional. Pulse la pestaña **Configuración de servidor** para configurar los elementos siguientes.

Configuración de plantilla de correo electrónico
Configure la plantilla para las notificaciones de correo electrónico.

Configuración de SMPT
Puede configurar IBM Data Risk Manager para que se envíen notificaciones de correo electrónico a los usuarios cuando Supervisión de actividad de base de datos (DAM) genere sucesos para realizar las acciones de reparación necesarias. Cuando está configurado SMTP, se puede obtener el envío de correo electrónico a los usuarios relevantes en actividades o tareas asociadas a un programa de este modo se integran sin problemas las funciones del Centro de acción de IBM Data Risk Manager.

Gestión de datos
Depurar problemas: si se selecciona, limpia las alertas o sucesos que ya no se utilizan en la base de datos del sistema. La configuración se establece en la duración por encima de la cual se deben depurar los datos. La duración se puede especificar en número de días, semanas o meses.

Limpiar registros de auditoría: si se selecciona, se limpian los registros de auditoría de la base de datos del sistema. Los registros de auditoría que IBM Data Risk Manager genera se acumulan a lo largo del tiempo y repercuten directamente en la utilización de espacio de disco. La configuración se establece en la duración por encima de la cual se deben depurar los datos. La duración se puede especificar en número de días, semanas o meses.

Valores de despliegue
Define el comportamiento operativo de todo el sistema.

Incluir CIAR	Seleccione esta opción para habilitar los criterios de confidencialidad, integridad, disponibilidad y fiabilidad para evaluar el riesgo de activos de información.
Admitir varios valores de taxonomía	Seleccione esta opción para admitir varios valores de taxonomía.
Tiempo de espera de transacción (en minutos)	Representa el periodo de tiempo máximo (en minutos) para la transacción de IBM Data Risk Manager antes de que se produzca el tiempo de espera.

Planificar definiciones de amenazas	Configure cuándo o con qué frecuencia las puntuaciones de riesgo se deben volver a calcular mediante el motor de riesgo.
Caducidad de la contraseña (en días)	Especifique el número máximo de días antes de que caduque una contraseña.
Política de contraseñas	Configure esta opción para establecer la política de complejidad de contraseñas.

Configuración de inicio de sesión único y LDAP

Se puede configurar IBM Data Risk Manager para establecer una conexión con un directorio LDAP o con un proveedor de servicio de inicio de sesión único. Debe tener en cuenta los puntos siguientes para establecer la conexión.

- El directorio LDAP o el servicio de inicio de sesión único deben estar en ejecución en un host que sea accesible para el servidor de IBM Data Risk Manager.
- Debe estar disponible una cuenta de LDAP con un nombre de usuario y contraseña para utilizarlos en IBM Data Risk Manager.
- Debe conocer el nombre de dominio completo (FQDN) del servidor LDAP.
- Debe conocer el número de puerto para que IBM Data Risk Manager se comunique con el servidor LDAP. El puerto predeterminado es 389.
- Para el inicio de sesión único, debe proporcionar el archivo XML `idp` o el URL del servicio de inicio de sesión único.
- Para un certificado autofirmado asociado al archivo `idp`, debe proporcionar la clave de certificado y la contraseña.

Para obtener más información acerca de la configuración del inicio de sesión único y LDAP, consulte "Integración de LDAP con IBM Data Risk Manager" en la página 100.

Integraciones entre productos

IBM Data Risk Manager se puede utilizar con otros productos de seguridad para obtener una solución integrada. Asegúrese de que los valores de configuración se han establecido correctamente para integrar varios adaptadores externos con IBM Data Risk Manager.

Integración de IBM Security Guardium con IBM Data Risk Manager

Puede utilizar IBM Data Risk Manager para identificar riesgos potenciales para la información empresarial confidencial utilizando las ofertas de Evaluación de vulnerabilidades de IBM Security Guardium, la Supervisión de la actividad de base de datos de IBM Security Guardium y la Supervisión del acceso a archivos.

El agente de Intercambio de integración de IBM Data Risk Manager (IntEx) se utiliza para consumir alertas de la Supervisión de actividad de base de datos (DAM), alertas de Supervisión de acceso a archivos (FAM), vulnerabilidades y la clasificación de datos de IBM Security Guardium.

Para integrar IBM Security Guardium con IBM Data Risk Manager, ejecute las tareas siguientes.

- Requisitos previos
  - Registro de IBM Security Guardium.
  - Importar plantillas de informes personalizadas a IBM Security Guardium.
  - Enviar el syslog de IBM Security Guardium al servidor de IBM Data Risk Manager.
  - Configurar las plantillas de informe de Syslog.
  - Configurar el escucha de IBM Data Risk Manager.
- Integración de IBM Security Guardium con IBM Data Risk Manager
- Consumo de alertas DAM y FAM en IBM Data Risk Manager

  - Creación de alertas DAM y FAM en IBM Security Guardium.
  - Flujo de tareas de la integración de alertas DAM y FAM en IBM Data Risk Manager.
  - Importar políticas DAM a IBM Data Risk Manager.
  - Correlación de alertas DAM y FAM de IBM Security Guardium con el panel de control de IBM Data Risk Manager.
- Consumo de los resultados de datos de clasificación en IBM Data Risk Manager
  - Importar políticas de clasificador a IBM Data Risk Manager.
  - Importar el archivo CSV de resultados del clasificador (datos de catálogo) a IBM Data Risk Manager.
  - Correlación de los datos de resultados de clasificación con la infraestructura en el panel de control de IBM Data Risk Manager.
- Activación e importación de la evaluación de vulnerabilidades a IBM Data Risk Manager
  - Creación de orígenes de datos de IBM Security Guardium en IBM Data Risk Manager.
  - Importar datos de contexto.
  - Importar pruebas de evaluación de vulnerabilidades (VA) de IBM Security Guardium.
  - Crear evaluación de IBM Security Guardium.
  - Ver el estado de la evaluación de IBM Security Guardium.
  - Ver los resultados de la exploración de evaluación de IBM Security Guardium.
  - Correlación de vulnerabilidades de IBM Security Guardium con la infraestructura en el panel de control de IBM Data Risk Manager.
  - Importar vulnerabilidades de IBM Security Guardium a IBM Data Risk Manager.
  - Importar vulnerabilidades como un archivo CSV a IBM Data Risk Manager.

Tareas de requisito previo
Debe completar las tareas de requisito previo para la integración de IBM Security Guardium con IBM Data Risk Manager

Para integrar IBM Security Guardium con IBM Data Risk Manager, realice las tareas de requisito previo siguientes. Asegúrese de que tiene la imagen de IBM Data Risk Manager Server o el build en el formato necesario, en función del entorno en el que está ejecutando la tarea de instalación. Para obtener más información sobre los requisitos previos de instalación, consulte “Requisitos previos de instalación” en la página 18.

- Registro de IBM Security Guardium.
- Importar plantillas de informes personalizadas a IBM Security Guardium.
- Enviar el syslog de IBM Security Guardium a IBM Data Risk Manager Server.
- Configurar las plantillas de informe de Syslog.
- Configurar el escucha de IBM Data Risk Manager.

Registro de IBM Security Guardium

Para acceder a los datos desde IBM Security Guardium utilizando las API REST, el servidor de IBM Data Risk Manager debe estar registrado en los dispositivos IBM Security Guardium. Se requiere un código de acceso para la solicitud de datos desde y para el dispositivo IBM Security Guardium. El código de acceso se genera mediante una clave secreta, que se obtiene de IBM Security Guardium, utilizando un usuario de IBM Security Guardium válido.

Si el gestor central gestiona todos los dispositivos de IBM Security Guardium, el gestor central debe estar registrado en IBM Data Risk Manager Server. Cuando se guardan los pasos de configuración para el gestor central, automáticamente se crean todos los dispositivos gestionados.

En el gestor central, utilice una sesión local autenticada mediante CLI para generar un secreto de cliente para la aplicación e inicie el mandato de API de IBM Security Guardium para registrar la aplicación de cliente.

```
$guard_host >grdapi register_oauth_client client_id=a3DRM
```

En la salida, ignore todo excepto: `client_secret` y `client_id`

```
ID=0
{"client_id":"a3Data Risk Manager","client_secret":"b683afdf-3383-480d-
a885-3cb400fd7919","grant_types":"password","scope":"read,write","redirect_uri":"https://
someApp"}
ok
```

Guarde la información de la clave de secreto para el futuro y para registrarse en IBM Data Risk Manager Server.

Importar plantillas de informes personalizadas a IBM Security Guardium

Para ver información acerca de los procesos de clasificación, los procesos de evaluación de vulnerabilidades, los resultados de la evaluación de vulnerabilidades y los resultados de clasificación que se ejecutan en dispositivos de IBM Security Guardium, se deben crear informes personalizados en todos los dispositivos de IBM Security Guardium. Estos informes personalizados habilitan los datos de acceso de IBM Data Risk Manager Server en dispositivos de IBM Security Guardium.

Nota: Se deben crear informes personalizados en los dispositivos de IBM Security Guardium en los que se ejecutan exploraciones de evaluación de vulnerabilidades y de clasificación.

Los diez informes de IBM Security Guardium completos recibidos desde IBM Data Risk Manager se pueden importar al gestor central de IBM Security Guardium.

1. En el gestor central de IBM Security Guardium. pulse **Gestionar** > **Gestión de datos** > **Importar definiciones**.
2. Cargue las diez definiciones exportadas (archivos `.sql`).
3. Importe las definiciones cargadas.

Envío del syslog de IBM Security Guardium a IBM Data Risk Manager Server

El servidor de IBM Data Risk Manager incluye un componente de escucha que supervisa las actividades y sucesos que intercalan los dispositivos del recopilador de IBM Security Guardium. El escucha de IBM Data Risk Manager agrega violaciones notificadas por los dispositivos del recopilador de IBM Security Guardium, basándose en las políticas de supervisión de actividades instaladas en los dispositivos. El escucha de IBM Data Risk Manager Server correlaciona los sucesos con la información adecuada y los activos de la infraestructura que se muestran en el panel de control de IBM Data Risk Manager.

El syslog de los dispositivos del recopilador de IBM Security Guardium, que supervisa el tráfico de base de datos desde los servidores de base de datos, se debe exportar a IBM Data Risk Manager Server. El proceso de la exportación del syslog a IBM Data Risk Manager se debe repetir en todos los dispositivos del recopilador de IBM Security Guardium que supervisan el tráfico de base de datos.

Nota: Las acciones asociadas a cada política de supervisión de actividades de base de datos deben tener una notificación SYSLOG.

En la consola de CLI del dispositivo del recopilador de IBM Security Guardium, ejecute el siguiente mandato para configurar el syslog en IBM Data Risk Manager Server.

```
store remotelog add non_encrypted all.all <dirección_ip>:<puerto> tcp
```

Verifique el almacén remoto del syslog mediante el mandato siguiente.

```
$ show remotelog
Remote syslog is in non-encrypted mode.
*.*    @@<IP_Data Risk Manager_Server>:<puerto>
ok
```

Para borrar la configuración remota del syslog, ejecute el mandato siguiente.

```
store remotelog clear <IP_servidor_remoto>:port tcp
```

Reinicie el núcleo de inspección y los motores del gestor central, si está presente el gestor central.

```
$ restart inspection-core
$ restart inspection-engines
```

Configurar las plantillas de informe de Syslog

Asimismo, para configurar los dispositivos del recopilador de IBM Security Guardium de modo que envíen el syslog al IBM Data Risk Manager remoto, se debe modificar la plantilla para el syslog. Para cada uno de los dispositivos de IBM Security Guardium, se puede editar la plantilla de mensajes en el perfil global del dispositivo.

1. Inicie sesión en la consola de la interfaz de usuario del dispositivo del recopilador de IBM Security Guardium.
2. Vaya a **Configuración** > **Herramientas y vistas**.
3. Seleccione **Perfil global**.
4. En la sección **Plantilla de mensaje** de **Perfil global**, copie y pegue la plantilla siguiente.

```
Alert:  %%ruleDescription
Category: %%category  Classification: %%classification   Severity: %%severity
Rule: # %%ruleID %%ruleDescription
Request Info:
  Session start: %%sessionStart
  Server Type: %%serverType
  Database Name: %%DBName
  Service Name: %%serviceName
  DB User: %%DBUser
  OS User: %%OSUser
  Server: %%serverIP (%%serverHostname)
  Server Port: %%serverPort
  Client: %%clientIP (%%clientHostname)
  Client PORT: %%clientPort
  Net Protocol: %%netProtocol
  DB Protocol: %%DBProtocol
  DB Protocol Version: %%DBProtocolVersion
Application Info:
  Application User Name: %%AppUserName
  Source Program: %%SourceProgram
  Authorization Code: %%AuthorizationCode
  Request Type: %%requestType
  Last Error: %%lastError
  SQL: %%SQLString
  SQL Status: %%SqlStatus
  SQL Timestamp: %%SQLTimestamp
To add to baseline: %%addBaselineConstruct
```

5. Pulse **Aplicar** para guardar la plantilla de mensaje del syslog.

Configurar el escucha de IBM Data Risk Manager

Consulte “Configuración del escucha de DAM y FAM de IBM Security Guardium” en la página 37 para obtener información sobre los pasos de configuración.

Configuración del escucha de DAM y FAM de IBM Security Guardium

Para consumir incidencias de IBM Security Guardium en IBM Data Risk Manager, debe configurar el escucha de Supervisión de actividad de base de datos (DAM) y el escucha de Supervisión de acceso a archivos (FAM).

Acerca de esta tarea

El archivo JAR del escucha se puede encontrar en `/home/a3user/Microservices`

Procedimiento

1. Abra una ventana de terminal.
2. Ejecute el mandato siguiente.

```
cd /home/a3user/Microservices/
java -jar A3AlbatrossListener.jar -s
```

3. Cuando se le solicite, especifique el número de su elección.

   Especifique 2 para editar la configuración del escucha.
   Especifique 1 para conectar con IBM Data Risk Manager Server
4. Especifique el URL de IBM Data Risk Manager Server con el formato siguiente.

```
https://<url-servidor>:<puerto>/albatross
```

5. Especifique el nombre de usuario y contraseña con los privilegios necesarios para conectar con IBM Data Risk Manager Server.
6. Seleccione la organización cuando se le solicite.

   Nota: Seleccionar la organización es obligatorio. El escucha correlaciona todos los registros de supervisión de la actividad de base de datos con las organizaciones seleccionadas.
7. Especifique la opción 2 para configurar los valores del puerto de syslog de IBM Security Guardium.

   Especifique el puerto de syslog donde los dispositivos de IBM Security Guardium envían los archivos de syslog a IBM Data Risk Manager Server – 9003.
8. Inicie el escucha de DAM/FAM de IBM Data Risk Manager ejecutando el mandato siguiente.

```
sudo service listener start
```

Integración de IBM Security Guardium con IBM Data Risk Manager
Configure IBM Data Risk Manager para que se comunique con IBM Security Guardium para utilizar su información de riesgo relacionada con los datos confidenciales en IBM Data Risk Manager para el análisis.

Antes de empezar

Asegúrese de que la clave secreta y el identificador de cliente están disponibles, lo que es necesario para establecer la conexión con IBM Security Guardium. Utilice la interfaz de línea de mandatos de IBM Security Guardium para generar una clave secreta para el servidor de IBM Data Risk Manager.

1. Inicie sesión en la interfaz de línea de mandatos de IBM Security Guardium.

```
# ssh cli@<url-dispositivo-guardium>
```

2. Genere una clave secreta para la aplicación e inicie el mandato de la API de Guardium para registrar la aplicación cliente.

```
guardium-hostname> grdapi register_oauth_client client_id=data-risk-manager
```

Acerca de esta tarea

El componente Modelador de contexto empresarial (BCM) de IBM Data Risk Manager proporciona el Asistente de integración de empresa para integrar IBM Security Guardium con IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager utilizando sus credenciales de usuario.
2. Pulse el icono de menú de aplicación .

3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
4. En la sección Configuración del adaptador, pulse el icono **Añadir adaptador de integración**  .
5. Seleccione **IBM Guardium** en la lista.
6. Para añadir una instancia de IBM Security Guardium, seleccione **IBM Guardium** en la lista de Configuración de adaptador.
7. En la sección Instancias de integración, pulse el icono **Añadir instancia** .
8. Establezca las siguientes opciones.

Opción	Descripción
Nombre	Especifique un nombre para la instancia de IBM Security Guardium.
URL	Especifique el URL para acceder a IBM Security Guardium, por ejemplo, `https://<IP-dispositivo Guardium/nombre de host:puerto>`.
Instancia de microservicio	Seleccione el agente necesario para la integración. Por ejemplo, `guardium-integration-intex`.
Tipo de Guardium	Seleccione cualquiera de los siguientes sistemas IBM Security Guardium para acceder a los objetos de datos e importarlos. • **Gestor central** • **Agregador** • **Recopilador**
Nombre de usuario	Especifique el nombre de usuario de IBM Security Guardium con el rol de administrador.
Contraseña	Especifique la contraseña para el nombre de usuario.
ID de cliente Guardium	Especifique el ID de cliente para conectarse a IBM Security Guardium.
Clave secreta de cliente Guardium	Especifique la clave secreta para establecer conexión con IBM Security Guardium.
Ejecutar VA	Seleccione esta opción para ejecutar la exploración de evaluación de vulnerabilidades.
Clasificador y evaluación de vulnerabilidades	Especifique el archivo de configuración para importar datos del servidor de integración a IBM Data Risk Manager para las evaluaciones de vulnerabilidad y clasificación de datos.
Canales de información	Especifique el archivo de configuración para recuperar los canales de información de syslog (sucesos de alertas) del servidor de integración. Estos sucesos de alertas se correlacionan con los activos de información y la infraestructura en IBM Data Risk Manager para visualizarlos en el panel de control.

9. Pulse **Guardar** para guardar los detalles de configuración.

Qué hacer a continuación

Para la instancia de adaptador que ha creado, puede probar la conectividad. Seleccione la instancia en la lista de **Instancias de integración** y, a continuación, pulse **Probar conexión** para probar si la

comunicación entre la instancia de IBM Security Guardium y el servidor IBM Data Risk Manager es satisfactoria.

Puede importar unidades gestionadas de la instancia del adaptador que ha creado. Seleccione la instancia del adaptador y, a continuación, pulse **Obtener unidades gestionadas**.

Consumo de alertas DAM y FAM en IBM Data Risk Manager
Debe ejecutar diferentes tareas para utilizar las alertas de Supervisión de actividad de base de datos (DAM) y de Supervisión de acceso a archivos (FAM) en IBM Data Risk Manager.

Para crear y utilizar alertas de DAM y FAM en IBM Data Risk Manager, ejecute las tareas siguientes.

- Creación de alertas DAM y FAM en IBM Security Guardium.
- Importar políticas DAM a IBM Data Risk Manager.
- Correlación de alertas DAM y FAM de IBM Security Guardium con el panel de control de IBM Data Risk Manager.

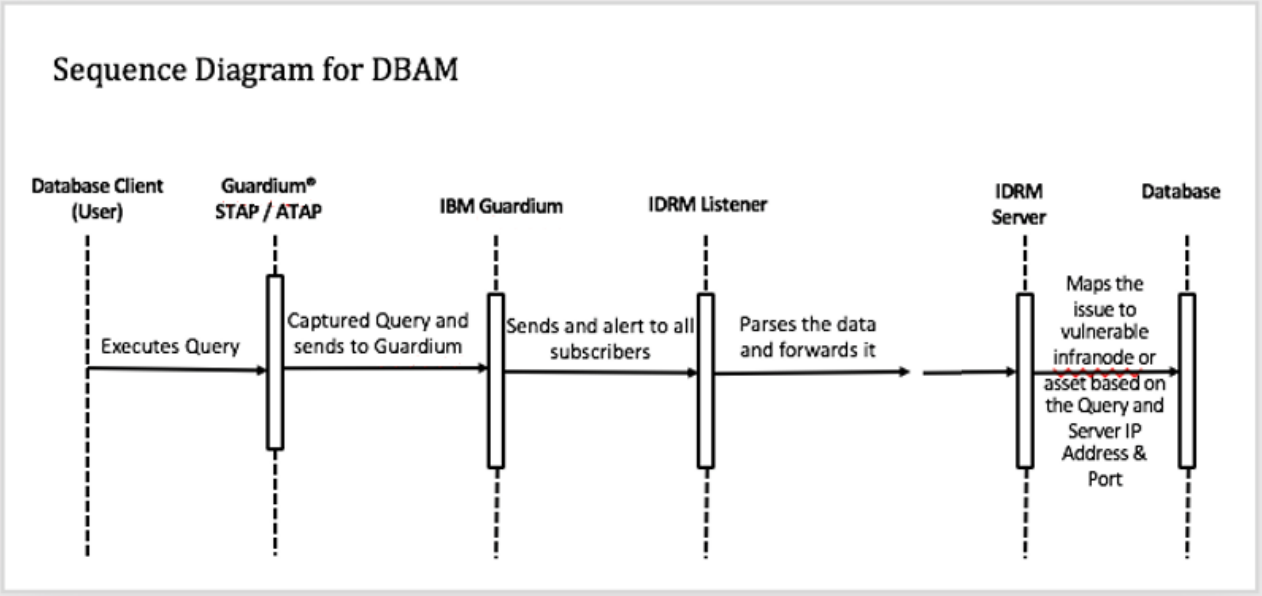
Creación de alertas DAM y FAM en IBM Security Guardium

Instale STAP en los servidores de base de datos donde se supervisan y evalúan los riesgos.

Las reglas de acceso de política DAM se crean en IBM Security Guardium y se despliegan en STAP. En función de una combinación de reglas, si desencadena una consulta SQL, STAP envía la consulta capturada a IBM Security Guardium. A continuación, IBM Security Guardium envía las alertas DAM mediante la interfaz de syslog al escucha de IBM Data Risk Manager que analiza los datos y los envía al servidor.

Flujo de tareas de la integración de alertas DAM y FAM en IBM Data Risk Manager

El diagrama siguiente muestra el flujo de trabajo de la integración de alertas DAM y FAM en IBM Data Risk Manager.



El servidor correlaciona el problema con el infranodo o activo vulnerable, basándose en la consulta y la dirección IP o puerto del servidor.

En el caso de FAM, se instala FTAP en el servidor de archivos. Cualquier acceso fraudulento al archivo sucede en el servidor, en función de la regla de política FAM que se ha desplegado en el dispositivo del recopilador. Las alertas FAM apropiadas se direccionan desde el servidor de archivos hasta IBM Security Guardium.

Importar políticas DAM a IBM Data Risk Manager

Para ver los pasos de importación de políticas DAM, consulte “Importar políticas de supervisión de actividad de base de datos a IBM Data Risk Manager” en la página 41.

Correlación de alertas DAM y FAM de IBM Security Guardium con el panel de control de IBM Data Risk Manager

1. Active IBM Security Guardium o una exploración no estructurada en cualquiera de los inventarios en los cuales está instalado STAP o FTAP.
2. Importe los datos de contexto y aplique los atributos de taxonomía.
3. Exporte el activo de información al panel de control.
4. Cuando se ejecuta la consulta SQL y satisface la regla DAM, las alertas DAM de IBM Security Guardium se direccionan al servidor IBM Data Risk Manager.
5. Cuando la actividad del archivo se ejecuta y satisface la regla FAM, las alertas FAM de IBM Security Guardium se direccionan al servidor IBM Data Risk Manager.
6. Las alertas DAM y FAM correspondientes se correlacionan con la infraestructura apropiada en IBM Data Risk Manager, que se pueden visualizar en la pestaña **Incidencias** en la página de detalles secundarios Activo de información. También se puede ver el número de alertas DAM y FAM en la pestaña **Infraestructura** que correlaciona el número de alertas con el inventario como base de datos, que tiene el icono de supervisor de STAP.

Importar políticas de supervisión de actividad de base de datos a IBM Data Risk Manager

Puede importar las políticas de supervisión de actividad de base de datos (DAM) IBM Security Guardium al inventario de IBM Data Risk Manager para clasificar datos y analizar riesgos.

Acerca de esta tarea

El icono de transacción  indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción  indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Políticas**.
4. Importar políticas.
   a) Pulse el icono **Descargar**  .
   b) En la ventana **Importar**, seleccione **Seguridad**.
   c) En la lista **Instancias**, seleccione una instancia de adaptador.
   d) Pulse **Importar**. Cuando se haya completado la operación de importación, se añadirán las políticas de IBM Security Guardium al inventario.
   e) Para renovar la lista de inventario de políticas, pulse el icono **Renovar**  .

Consumo de los resultados de los datos de clasificación en IBM Data Risk Manager

Debe ejecutar diferentes tareas para utilizar los resultados de los datos de clasificación en IBM Data Risk Manager.

Para utilizar los resultados de los datos de clasificación en IBM Data Risk Manager, ejecute las tareas siguientes.

- Importar políticas de clasificador a IBM Data Risk Manager.
- Importar el archivo CSV de resultados del clasificador (datos de catálogo) a IBM Data Risk Manager.
- Correlación de los datos de resultados de clasificación con la infraestructura en el panel de control de IBM Data Risk Manager.

Importar políticas de clasificador a IBM Data Risk Manager

Puede importar políticas de clasificador si se han creado las políticas en IBM Security Guardium. Para ver los pasos sobre cómo importar políticas, consulte "Importar políticas de clasificador a IBM Data Risk Manager" en la página 42.

Importar el archivo CSV de resultados del clasificador (datos de catálogo) a IBM Data Risk Manager.

Para ver los pasos para importar el archivo CSV de resultados del clasificador (datos de catálogo) a IBM Data Risk Manager, consulte "Importar el archivo CSV de resultados del clasificador (datos de catálogo) a IBM Data Risk Manager" en la página 43

Correlación de los datos de resultados de clasificación con la infraestructura en el panel de control de IBM Data Risk Manager.

1. Active una metaexploración de IBM Security Guardium en cualquiera de los sistemas donde se haya creado el inventario de IBM Security Guardium.
2. Importe los datos de contexto y aplique los atributos de taxonomía.
3. Exporte el activo de información al panel de control de IBM Data Risk Manager.
4. Se correlacionan los resultados del clasificador correspondientes con la infraestructura adecuada en IBM Data Risk Manager. Se pueden ver los resultados en Detalles del activo de información, en el widget Infraestructura que muestra el porcentaje del activo de datos.

Importar políticas de clasificador a IBM Data Risk Manager

Puede importar las políticas de clasificador de dispositivos de IBM Security Guardium al inventario de IBM Data Risk Manager para clasificar datos y analizar riesgos.

Acerca de esta tarea

El icono de transacción  indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción  indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Políticas**.
4. Importe las políticas de clasificador.
   a) Pulse el icono **Descargar**  .
   b) En la ventana **Importar**, seleccione **Clasificador**.
   c) En la lista **Instancias**, seleccione una instancia de adaptador.

d) Pulse **Importar**. Cuando se haya completado la operación de importación, se añadirán las políticas de IBM Security Guardium al inventario.

e) Para renovar la lista de inventario de políticas, pulse el icono **Renovar**  .

Importar el archivo CSV de resultados del clasificador (datos de catálogo) a IBM Data Risk Manager

Utilice el componente Modelador de contexto empresarial de IBM Data Risk Manager para importar los resultados del clasificador como un archivo CSV a IBM Data Risk Manager.

Antes de empezar

Asegúrese de que los datos de contexto empresarial estén disponibles para importarlos.

Puede descargar las plantillas de ejemplo en: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**.
4. Habilite el botón de conmutación **Datos de catálogo**.
5. Seleccione **Clasificación**.
6. Pulse **Elegir archivo** para localizar y seleccionar el archivo.
7. Pulse **Cargar**.
   Los datos se visualizan para su verificación.
8. Pulse **Importar**.

Activación e importación de la evaluación de vulnerabilidades a IBM Data Risk Manager

Debe ejecutar varias tareas para activar e importar la evaluación de vulnerabilidades a IBM Data Risk Manager.

Para activar e importar la evaluación de vulnerabilidades a IBM Data Risk Manager, ejecute las tareas siguientes.

- Creación de orígenes de datos de IBM Security Guardium en IBM Data Risk Manager.
- Importar datos de contexto.
- Importar pruebas de vulnerabilidades de IBM Security Guardium.
- Crear evaluación de IBM Security Guardium.
- Ver el estado de la evaluación de IBM Security Guardium.
- Ver los resultados de la exploración de evaluación de IBM Security Guardium.
- Correlación de vulnerabilidades de IBM Security Guardium con la infraestructura en el panel de control de IBM Data Risk Manager.
- Importar vulnerabilidades de IBM Security Guardium a IBM Data Risk Manager.
- Importar vulnerabilidades como un archivo CSV a IBM Data Risk Manager.

Creación de orígenes de datos de IBM Security Guardium en IBM Data Risk Manager

Para ver los pasos sobre cómo crear los orígenes de datos, consulte “Adición de orígenes de datos de IBM Security Guardium” en la página 44.

Importar datos de contexto

Importe datos de contexto. Asegúrese de que los datos de contexto se guarden correctamente y que los atributos se correlacionen correctamente con el inventario adecuado que se ha creado anteriormente. Para obtener más información sobre cómo importar los datos de contexto, consulte "Correlación de datos de contexto empresarial" en la página 106.

Nota: Se puede crear el inventario en IBM Data Risk Manager proporcionando el nombre del origen de datos y el tipo en la hoja de datos de contexto `Base de datos`.

Importar pruebas de evaluación de vulnerabilidades (VA) de IBM Security Guardium

Para ver los pasos para importar las pruebas VA, consulte "Importar pruebas de evaluación de vulnerabilidades de IBM Security Guardium" en la página 45.

Crear evaluación de IBM Security Guardium

Para ver los pasos para crear una evaluación, consulte "Crear y activar una exploración de evaluación de vulnerabilidades" en la página 46.

Ver el estado de la evaluación de IBM Security Guardium

Para ver los pasos sobre cómo ver el estado, consulte "Ver el estado de la exploración " en la página 57.

Ver los resultados de la exploración de evaluación de IBM Security Guardium

Para ver los pasos sobre cómo ver los resultados de la exploración, consulte "Ver los resultados de la exploración de evaluación de vulnerabilidades de IBM Security Guardium" en la página 47.

Correlación de vulnerabilidades de IBM Security Guardium con la infraestructura en el panel de control de IBM Data Risk Manager

Cuando se completan los resultados de la exploración en el panel de control Vulnerabilidad, puede ver los resultados de la exploración de vulnerabilidades en el panel de control de IBM Data Risk Manager. Pulse la página secundaria Activo de información para ver las vulnerabilidades del inventario de puntos finales de IBM Security Guardium. El recuento de vulnerabilidades de la infraestructura se muestra en el widget Infraestructura.

Importar vulnerabilidades de IBM Security Guardium a IBM Data Risk Manager

Para ver los pasos sobre cómo importar vulnerabilidades, consulte Importar exploraciones de vulnerabilidades.

Importar vulnerabilidades como un archivo CSV a IBM Data Risk Manager

Puede importar vulnerabilidades como un archivo CSV a IBM Data Risk Manager. Para ver los pasos sobre cómo importar el archivo CSV, consulte Importar exploraciones de vulnerabilidades.

Reparación de vulnerabilidades

Cuando se identifican las vulnerabilidades mediante exploraciones, se deben llevar a cabo acciones de reparación para evaluar la exposición de riesgo correcta para el activo de información. Para ver los pasos sobre cómo definir acciones de reparación, consulte "Creación de una actividad para reparar vulnerabilidades " en la página 48.

Adición de orígenes de datos de IBM Security Guardium

Puede añadir orígenes de datos de IBM Security Guardium en el inventario de IBM Data Risk Manager para que los datos estén disponibles para el análisis de riesgos y acciones.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security Guardium. Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium con IBM Data Risk Manager" en la página 38.

Antes de crear un origen de datos, debe tener en cuenta los parámetros de conexión de base de datos para el origen de datos al que desee conectarse.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.
4. Para añadir un origen de datos de IBM Security Guardium, pulse el icono **Añadir origen de datos**  .
5. En la página **Añadir origen de datos**, establezca las opciones siguientes y pulse **Añadir**.

Opción	Descripción
Tipo de servidor	El tipo de servidor de base de datos que desea utilizar. Por ejemplo, MySQL.
Nombre de origen de datos	Nombre exclusivo para el origen de datos.
Dirección IP	Dirección IP del servidor de bases de datos.
Puerto	Número de puerto de escucha del origen de datos.
Nombre de base de datos	Nombre de la base de datos.
Adaptador	Nombre de instancia de IBM Security Guardium. Por ejemplo, `Guardium_Adapter`.
Agentes	Nombre de agente para conectarse a la base de datos.
Nombre de usuario	El nombre del usuario para conectarse a la base de datos.
Contraseña	Contraseña para el nombre de usuario de base de datos.
Cifrado	Estado de cifrado del servidor de origen de datos.
Supervisión	El estado del agente de supervisión de base de datos como, por ejemplo, S-TAP.
URL personalizado	Serie de URL personalizado para conectarse al origen de datos.
Ubicación geográfica	Ubicación geográfica del origen de datos.

El origen de datos que ha añadido aparece listado en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Base de datos**.

Importar pruebas de evaluación de vulnerabilidades de IBM Security Guardium

Importe las pruebas de evaluación de vulnerabilidades de IBM Security Guardium (VA) a IBM Data Risk Manager para analizar los datos.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de navegación de la aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Pruebas VA**.
4. Para descargar plantillas de exploración, pulse el icono **Descargar** .
5. En la ventana **Importar**, seleccione una instancia de adaptador para IBM Security Guardium.
6. Pulse **Importar**. Cuando la operación de importación se haya completado, las pruebas VA se añaden al inventario.
7. Para renovar la lista de inventario de pruebas VA, pulse el icono **Renovar** .

Crear y activar una exploración de evaluación de vulnerabilidades

Utilice el componente Gestión de vulnerabilidades de IBM Data Risk Manager para crear y ejecutar la exploración de evaluación en IBM Security Guardium para identificar vulnerabilidades en bases de datos.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security Guardium. Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium con IBM Data Risk Manager" en la página 38.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Pulse **Gestión de vulnerabilidades**.
4. Seleccione un programa de la lista.
5. Pulse **Crear nueva evaluación**.
6. En la página **Crear nueva evaluación**, establezca las opciones siguientes y pulse **Crear evaluación**.

Opción	Descripción
Nombre de evaluación	Nombre de la evaluación de vulnerabilidades de IBM Security Guardium.
Tipo de exploración	El tipo de exploración, por ejemplo, `Explorador de base de datos`.
Plataforma	Selección de tipo de base de datos para ejecutar el proceso de evaluación de vulnerabilidades.
Ejecutar el	Instancia del adaptador de IBM Security Guardium para ejecutar el proceso de evaluación de vulnerabilidades. La lista solo contiene las instancias para las cuales está seleccionada la opción **Ejecutar VA** cuando se crea la instancia de integración.

7. En **Ámbito de evaluación**, añada orígenes de datos a la transacción en función del ámbito o de los últimos días de exploración. Puede añadir varios orígenes de datos.
8. Pulse **Añadir ámbito a transacción**.
9. Seleccione las pruebas de vulnerabilidad en la lista y pulse **Guardar**.
10. En **Transacciones pendientes** en la vista Transacción, pulse el icono **Iniciar proceso** .
11. Seleccione **Explorar ahora**.

    Para planificar la exploración más tarde, seleccione **Explorar después**.

Para guardar los detalles de la transacción tras la finalización del proceso en **Transacciones pendientes** para su reutilización, seleccione **Réplica**.

12. Para iniciar el proceso, pulse el icono **Activar evaluación** .

Ver los resultados de la exploración de evaluación de vulnerabilidades de IBM Security Guardium

Utilice el componente Evaluación de vulnerabilidades de IBM Data Risk Manager para ver los resultados de la exploración de evaluación de vulnerabilidades para un análisis y acciones adicionales.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Pulse **Gestión de vulnerabilidades**.
4. Pulse **Ver resultados**.
5. Pulse el icono Filtro en **Orígenes de datos VA** y seleccione el tipo de adaptador, por ejemplo, `IBM Guardium`.
6. Para la evaluación seleccionada, pulse el número para **Aprobado**, **Error** u **Otros** para visualizar los resultados en la página **Resultados de prueba de vulnerabilidades**.
7. Para ver los resultados según la plataforma, pulse **Plataformas VA**.

Importar vulnerabilidades de IBM Security Guardium a IBM Data Risk Manager

Puede importar exploraciones de vulnerabilidades desde IBM Security Guardium al inventario de IBM Data Risk Manager para el análisis de riesgos.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security Guardium. Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium con IBM Data Risk Manager" en la página 38.

Acerca de esta tarea

El icono de transacción indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Exploraciones de datos**.
4. Importe las exploraciones de datos.
   a) Pulse el icono **Descargar** .
   b) En la ventana **Importar**, seleccione **Evaluación de vulnerabilidad**.
   c) Desde la lista **Adaptador**, seleccione **IBM Guardium**.
   d) En la lista **Instancias**, seleccione una instancia de adaptador. Puede seleccionar hasta tres instancias.

e) Seleccione la fecha a partir de la cual tendrá que extraer exploraciones de evaluación de vulnerabilidades desde IBM Security Guardium.

f) Pulse **Importar**. Cuando se haya completado la operación de importación, las exploraciones de evaluación de vulnerabilidades de IBM Security Guardium se añaden al inventario.

5. En la página **Exploraciones de datos**, puede ver las exploraciones que ha importado ahora.
6. Para renovar la lista de inventario de exploraciones de datos, pulse el icono **Renovar** .
7. De forma alternativa, para ver los resultados de exploración después de la operación de importación, vaya a **Centro de control y mandatos de seguridad** > **Inicio**.

Importar vulnerabilidades como un archivo CSV a IBM Data Risk Manager

Utilice el componente Modelador de contexto empresarial de IBM Data Risk Manager para importar las vulnerabilidades como un archivo CSV a IBM Data Risk Manager.

Antes de empezar

Asegúrese de que los datos de contexto empresarial estén disponibles para importarlos.

Puede descargar las plantillas de ejemplo en: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**.
4. Habilite el botón de conmutación **Datos de catálogo**.
5. Seleccione **Vulnerabilidad**.
6. Pulse **Elegir archivo** para localizar y seleccionar el archivo.
7. Pulse **Cargar**.

   Los datos se visualizan para su verificación.
8. Pulse **Importar**.

Creación de una actividad para reparar vulnerabilidades

Utilice el componente Gestión de vulnerabilidades de IBM Data Risk Manager para ver y reparar vulnerabilidades. Cuando se identifican las vulnerabilidades mediante exploraciones, se deben llevar a cabo acciones de reparación para evaluar la exposición de riesgo correcta para el activo de información.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Pulse **Gestión de vulnerabilidades**.
4. Vaya a **Vista de resultados**.
5. Pulse **Orígenes de datos VA**.
6. Pulse el icono de filtro en **Orígenes de datos VA** y seleccione el tipo de adaptador, por ejemplo, `IBM QRadar`.
7. De forma alternativa, puede seleccionar un origen de datos basado en la plataforma.

   a) Pulse **Plataformas VA**.

b) Seleccione una plataforma y pulse el icono de base de datos  para seleccionar el origen de datos.

8. Para un origen de datos seleccionado, pulse el número para **Error** para mostrar los resultados en la página **Resultados de la prueba de vulnerabilidades**.
9. Pulse el icono de flecha hacia abajo  para seleccionar el nivel de gravedad.
10. Pulse el icono **Reparación**  .
11. Pulse **Sí** para crear acciones de reparación.
12. En la ventana **Crear actividad de reparación**, especifique la información necesaria. Si el origen de datos procede de ServiceNow, puede publicar la actividad como incidencia en ServiceNow para la gestión de reparaciones.
13. Pulse **Crear**.

    En la página **Resultados de la prueba de vulnerabilidades**, en **Actividad**, puede ver los detalles de actividad si la fecha de finalización de la actividad es mayor que la fecha de ejecución de los resultados de prueba.

Qué hacer a continuación

Puede ver y gestionar las actividades de reparación que ha definido en las áreas siguientes.

Centro de acción de IBM Data Risk Manager

- Pulse el icono de menú de aplicación  .
- Pulse **Centro de acción**.

Para obtener más información sobre el Centro de acción, consulte "Centro de acción" en la página 151.

La ventana Detalles de activo en el panel de control de IBM Data Risk Manager

- Pulse el icono de menú de aplicación  .
- Pulse **Panel de control**.
- En la ventana **Conjunto de activos de información**, pulse el icono de flecha  en el activo para ver los detalles del activo.
- En la ventana **Detalles de activo**, pulse **Infraestructura** > **Vulnerabilidades**.
- Para ver elementos de acción, seleccione el nodo de infraestructura y pulse **Elementos de acción**.

Exportación de orígenes de datos IBM Security Guardium limpios al panel de control

Puede exportar directamente el origen de datos de IBM Security Guardium limpio al panel de control de IBM Data Risk Manager. Debe importar la exploración de clasificador desde IBM Security Guardium donde se ejecuta la exploración en el origen de datos que desea exportar.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security Guardium. Para obtener más información sobre los pasos de integración, consulte "Integración de IBM Security Guardium con IBM Data Risk Manager" en la página 38.

Asegúrese de que las exploraciones del clasificador IBM Security Guardium se han importado al inventario de IBM Data Risk Manager. Para obtener más información sobre cómo importar la exploración, consulte "Importación de exploraciones de clasificador desde IBM Security Guardium" en la página 143.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Exploraciones de datos**.
4. Seleccione la exploración de clasificador, que se ejecuta en el origen de datos que desea exportar al panel de control de IBM Data Risk Manager.
5. Pulse el icono de exportación  .
6. Pulse **Sí** para confirmar la operación de exportación.

   El icono de exportación  en la exploración de datos seleccionada indica que la exploración se ha exportado al panel de control.

   Pulse el icono de información para ver el número de orígenes de datos, tablas y columnas que están asociados a la exploración seleccionada.
7. Seleccione el programa en la lista.
8. Vea el origen de datos que ha exportado al panel de control de IBM Data Risk Manager.
   a) Vaya a **Modelador de contexto empresarial** > **Panel de control**.
   b) Pulse **Programa** para seleccionar el programa.
   c) Pulse **Panel de control** para ver el activo.

Supervisión de actividad de archivos
La supervisión de actividad de archivos (FAM) descubre los datos confidenciales en los servidores. El descubrimiento de datos incluye la recopilación de metadatos y las titularidades de los archivos y carpetas.

FAM incluye las actividades siguientes:

- Clasifica el contenido utilizando definiciones predefinidas o definidas por el usuario.
- Configura reglas y políticas sobre el acceso a datos y las acciones que se deben llevar a cabo cuando se cumplen las reglas.
- Se adapta a los crecientes volúmenes de datos y a la expansión de los requisitos empresariales.
- Proporciona un amplio soporte heterogéneo a través de todos los sistemas de datos populares.

FAM consta de las funciones siguientes:

- Realiza el seguimiento de las actividades de usuario, como la modificación o la supresión de contenido en archivos y carpetas.
- Realiza el seguimiento de todas las actividades relacionadas con la base de datos en archivos y carpetas.
- Notifica a los administradores y propietarios acerca de las operaciones de base de datos que se realizan en los archivos y las carpetas.

Integración de IBM QRadar Security Intelligence Platform con IBM Data Risk Manager

Los sucesos que se marcan como delito en IBM QRadar Security Intelligence Platform se importan a IBM Data Risk Manager. Estos sucesos se consumen como amenaza en IBM Data Risk Manager y, a continuación, se correlacionan con la infraestructura adecuada para análisis y evaluaciones.

El agente de Intercambio de integración de IBM Data Risk Manager (IntEx) se utiliza para consumir vulnerabilidades de aplicaciones de IBM Security AppScan EnterpriseIBM QRadar Security Intelligence Platform.

Para obtener más información sobre los requisitos previos de instalación, consulte “Requisitos previos de instalación” en la página 18.

Para consumir delitos de IBM QRadar Security Intelligence Platform en IBM Data Risk Manager y para importar la evaluación de vulnerabilidades de IBM QRadar Security Intelligence Platform a IBM Data Risk Manager, ejecute las tareas siguientes.

- Consumir delitos de IBM QRadar Security Intelligence Platform en IBM Data Risk Manager.
  - Crear delitos en IBM QRadar Security Intelligence Platform.
  - Flujo de trabajo de integración de delitos en IBM Data Risk Manager.
  - Integración de IBM QRadar Security Intelligence Platform con IBM Data Risk Manager.
  - Configuración del escucha de IBM QRadar Security Intelligence Platform SIEM.
  - Correlación de delitos de IBM QRadar Security Intelligence Platform en el panel de control de IBM Data Risk Manager.
- Activación e importación de la evaluación de vulnerabilidades de IBM QRadar Security Intelligence Platform a IBM Data Risk Manager.
  - Creación del inventario de punto final de IBM Data Risk Manager.
  - Importar datos de contexto.
  - Crear evaluación de puntos finales.
  - Ver estado de la exploración de evaluación de puntos finales.
  - Ver resultados de la exploración de evaluación de puntos finales.
  - Correlación de vulnerabilidades con la infraestructura en el panel de control de IBM Data Risk Manager.
  - Importar vulnerabilidades de puntos finales a IBM Data Risk Manager.

Crear delitos en IBM QRadar Security Intelligence Platform

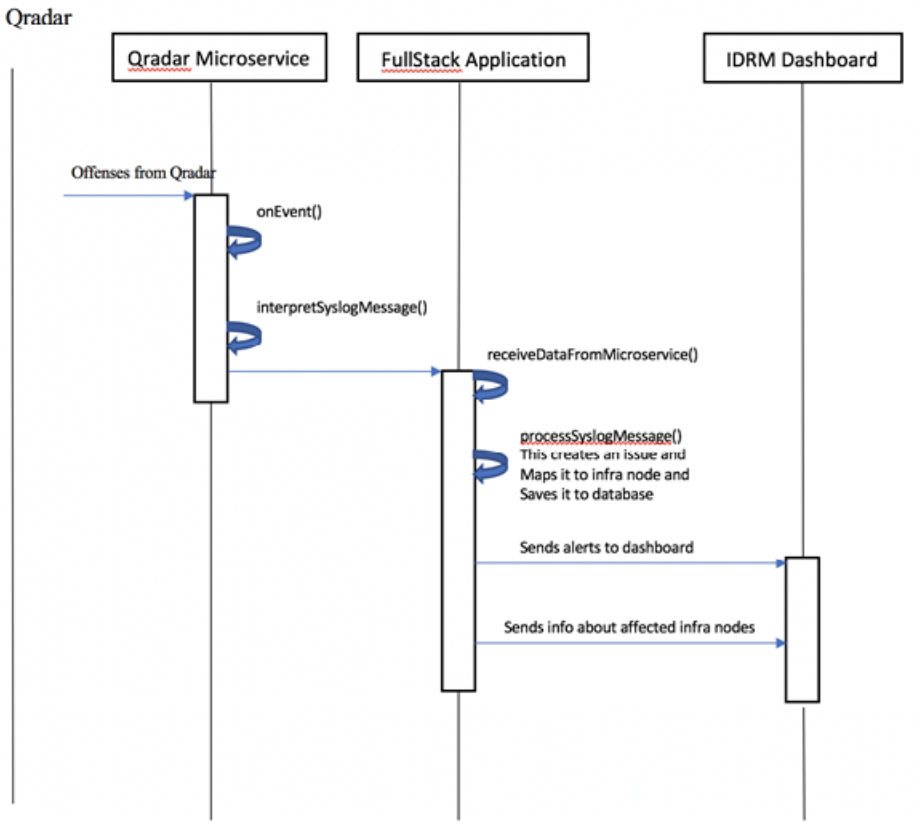
Para recopilar sucesos desde IBM QRadar Security Intelligence Platform, instale el agente de recopilación Win en el sistema Windows. Habilite syslog para sistemas que no sean Windows

Después de instalar el agente de recopilación en sistemas Windows y de configurar IBM QRadar Security Intelligence Platform creando un origen de registro, los sucesos están disponibles como una actividad de registro.

Flujo de trabajo de integración de delitos en IBM Data Risk Manager

IBM QRadar Security Intelligence Platform crea el delito basándose en la regla personalizada que se ha creado en el dispositivo sobre un factor de riesgo específico, por ejemplo la hora. Se puede crear un delito si los sucesos se producen en esas ventanas de tiempo específicas.

Cuando estos delitos se consumen en IBM Data Risk Manager, el micro servicio IBM Data Risk Manager SIEM, interpreta estos mensajes del syslog y los envía al servidor. A continuación, se procesan los datos, se crea un problema y se correlaciona con la infraestructura adecuada. El siguiente diagrama muestra el flujo de trabajo de los delitos.



Integración de IBM QRadar Security Intelligence Platform con IBM Data Risk Manager.

Configure IBM Data Risk Manager para que se comunique con IBM QRadar Security Intelligence Platform. Para obtener información sobre los pasos de configuración, consulte Integración de IBM QRadar Security Intelligence Platform con IBM Data Risk Manager.

Configuración del escucha de IBM QRadar Security Intelligence Platform SIEM

Para consumir delitos de IBM QRadar Security Intelligence Platform en IBM Data Risk Manager, debe configurar el escucha de SIEM. Consulte "Configuración del escucha de IBM QRadar Security Intelligence Platform SIEM" en la página 55 para obtener información sobre los pasos de configuración.

Correlación de delitos de IBM QRadar Security Intelligence Platform en el panel de control de IBM Data Risk Manager

Para correlacionar delitos de IBM QRadar Security Intelligence Platform con la infraestructura del panel de control de IBM Data Risk Manager, ejecute los pasos siguientes.

1. Desencadene la exploración en cualquier inventario en que este instalado el agente de recopilación Win.
2. Importe los datos de contexto, aplique los atributos de taxonomía y exporte el activo de información al panel de control de IBM Data Risk Manager.

   Cuando esté activo el escucha y se hayan configurado las reglas personalizadas adecuados en IBM QRadar Security Intelligence Platform, se generarán los delitos y se enviarán a IBM Data Risk Manager.
3. Los delitos que se correlacionan con la infraestructura en el panel de control de IBM Data Risk Manager, se pueden ver en la pestaña **Delitos** de la página de detalles secundaria **Activo de información**. También se puede ver el número de delitos en la pestaña **Infraestructura** asociada al número de alertas, siendo el inventario el punto final.

Creación del inventario de punto final en IBM Data Risk Manager

Añada el inventario de punto final de IBM QRadar Security Intelligence Platform a IBM Data Risk Manager. Para ver los pasos sobre cómo añadir el inventario, consulte "Adición de orígenes de datos de IBM QRadar Security Intelligence Platform" en la página 55.

Importar datos de contexto

Importe datos de contexto. Asegúrese de que los datos de contexto se guarden correctamente y que los atributos se correlacionen correctamente con el inventario adecuado que se ha creado anteriormente. Para obtener más información sobre cómo importar los datos de contexto, consulte "Correlación de datos de contexto empresarial" en la página 106.

Nota: Se puede crear el inventario en IBM Data Risk Manager proporcionando el nombre del origen de datos y el tipo en la hoja de datos de contexto `Base de datos`.

Crear evaluación de puntos finales

Utilice el componente Evaluación de vulnerabilidades de IBM Data Risk Manager para crear la evaluación de puntos finales. Para ver los pasos sobre cómo crear la evaluación de puntos finales, consulte "Crear y activar una exploración de evaluación de puntos finales" en la página 56.

Ver estado de la exploración de evaluación de puntos finales

Puede ver el estado de la exploración de evaluación de aplicaciones para continuar con un análisis y acciones adicionales. Para ver los pasos sobre cómo ver el estado de la exploración, consulte Ver estado de la exploración.

Ver resultados de la exploración de evaluación de puntos finales

Vea los resultados de la exploración de evaluación de puntos finales para realizar un análisis y acciones adicionales. Para ver los pasos sobre cómo ver los resultados de la exploración, consulte Ver resultados de la exploración.

Correlación de vulnerabilidades con la infraestructura en el panel de control de IBM Data Risk Manager

Cuando se ha completado correctamente la exploración de la evaluación de aplicaciones, puede ver los resultados de la exploración de vulnerabilidades en el panel de control de IBM Data Risk Manager. Vaya a la página secundaria Activo de información para ver las vulnerabilidades del inventario de puntos finales. El recuento de vulnerabilidades de la infraestructura se muestra en el widget Infraestructura. Para obtener más información sobre el panel de control, consulte "Panel de control de IBM Data Risk Manager" en la página 177.

Importar vulnerabilidades de puntos finales a IBM Data Risk Manager

Importe las exploraciones de vulnerabilidades desde los dispositivos de IBM QRadar Security Intelligence Platform al inventario de IBM Data Risk Manager para clasificar los datos y analizar riesgos. Para ver los pasos sobre cómo importar la exploración, consulte Importar exploraciones de vulnerabilidades.

Nota: Cuando importa las exploraciones, también se importan los orígenes de datos y los resultados de las importaciones.

Importar vulnerabilidades de puntos finales a IBM Data Risk Manager

Puede importar vulnerabilidades como un archivo CSV a IBM Data Risk Manager. Para ver los pasos sobre cómo importar el archivo CSV, consulte Importar vulnerabilidades como archivo CSV a IBM Data Risk Manager.

Reparación de vulnerabilidades

Cuando se identifican las vulnerabilidades mediante exploraciones, se deben llevar a cabo acciones de reparación para evaluar la exposición de riesgo correcta para el activo de información. Para ver los pasos sobre cómo definir acciones de reparación, consulte “Creación de una actividad para reparar vulnerabilidades ” en la página 48.

Integración de IBM QRadar Security Intelligence Platform con IBM Data Risk Manager

Configure IBM Data Risk Manager para que se comunique con IBM QRadar Security Intelligence Platform para utilizar su información de riesgo relacionada con los datos confidenciales en IBM Data Risk Manager para el análisis.

Acerca de esta tarea

El componente Modelador de contexto empresarial (BCM) de IBM Data Risk Manager proporciona el Asistente de integración de empresa para integrar IBM QRadar Security Intelligence Platform con IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
4. En la sección Configuración del adaptador, pulse el icono **Añadir adaptador de integración** .
5. Seleccione **IBM QRadar** en la lista.
6. Para añadir una instancia de IBM QRadar Security Intelligence Platform, seleccione **IBM QRadar** en la lista de Configuración de adaptador.
7. En la sección Instancias de integración, pulse el icono **Añadir instancia** .
8. Establezca las siguientes opciones.

Opción	Descripción
Nombre	Especifique un nombre para la instancia de IBM QRadar Security Intelligence Platform.
URL	Especifique el URL para acceder a IBM QRadar Security Intelligence Platform, por ejemplo, `https://<IP-aplicación qradar/nombre de host:puerto>`.
Instancia de microservicio	Seleccione el agente necesario para la integración.
Nombre de usuario	Especifique el nombre de usuario de IBM QRadar Security Intelligence Platform con el rol de administrador.
Contraseña	Especifique la contraseña para el nombre de usuario.
Clasificador y evaluación de vulnerabilidades	Especifique el archivo de configuración para importar datos del servidor de integración a IBM Data Risk Manager para las evaluaciones de vulnerabilidad y clasificación de datos.
Canales de información	Especifique el archivo de configuración para recuperar los canales de información de syslog (sucesos de alertas) del servidor de integración. Estos sucesos de alertas se correlacionan con los activos de información y la infraestructura en IBM Data Risk Manager para visualizarlos en el panel de control.

9. Pulse **Guardar** para guardar los detalles de configuración.

Qué hacer a continuación
Para la instancia de adaptador que ha creado, puede probar la conectividad. Seleccione la instancia en la lista de **Instancias de integración** y, a continuación, pulse **Probar conexión** para probar si la comunicación entre la instancia de IBM QRadar Security Intelligence Platform y el servidor IBM Data Risk Manager es satisfactoria.

Configuración del escucha de IBM QRadar Security Intelligence Platform SIEM
Para consumir delitos de IBM QRadar Security Intelligence Platform en IBM Data Risk Manager, debe configurar el escucha de SIEM.

Acerca de esta tarea

El archivo JAR del escucha se puede encontrar en: `/home/a3user/Micro services`

Procedimiento

1. Abra una ventana de terminal.
2. Ejecute el mandato siguiente.

```
cd /home/a3user/Microservices/
java -jar A3EurekaQradar.jar -s
```

3. Cuando se le solicite, especifique el número de su elección.

   Especifique 2 para editar la configuración del escucha.
   Especifique 1 para conectar con IBM Data Risk Manager Server
4. Especifique el URL de IBM Data Risk Manager Server con el formato siguiente.

```
https://<url-servidor>:<puerto>/albatross
```

5. Especifique el nombre de usuario y contraseña con los privilegios necesarios para conectar con IBM Data Risk Manager Server.
6. Seleccione la organización cuando se le solicite.

   Nota: Seleccionar la organización es obligatorio. El escucha correlaciona todos los registros de supervisión de la actividad de base de datos con las organizaciones seleccionadas.
7. Especifique la opción 2 para configurar los valores del puerto de syslog de IBM QRadar Security Intelligence Platform.

   Especifique el puerto de syslog donde los dispositivos de IBM QRadar Security Intelligence Platform envían los archivos de syslog a IBM Data Risk Manager Server – 9000.
8. Inicie el escucha de IBM Data Risk Manager QRadar ejecutando el mandato siguiente.

```
sudo service qradar start
```

Adición de orígenes de datos de IBM QRadar Security Intelligence Platform
Puede añadir orígenes de datos IBM QRadar Security Intelligence Platform en el inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con IBM QRadar Security Intelligence Platform. Para obtener más información sobre la integración, consulte IntegraciónIBM QRadar Security Intelligence Platform con IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .

3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.
4. Para añadir un origen de datos de IBM QRadar Security Intelligence Platform, pulse el icono **Añadir origen de datos** ⊕.
5. En la página **Añadir origen de datos**, establezca las opciones siguientes y pulse **Añadir**.

Opción	Descripción
Tipo de servidor	El tipo de servidor de origen de datos que desea utilizar, por ejemplo, `Servidor`.
Nombre de origen de datos	Nombre del origen de datos.
Dirección IP	La dirección IP del servidor de origen de datos.
Adaptador	Nombre de instancia de IBM QRadar Security Intelligence Platform. Por ejemplo, `Qradar_Adapter`.
Agentes	Nombre de agente para conectarse al origen de datos.
Nombre de usuario	Nombre del usuario.
Contraseña	Contraseña para el nombre de usuario.
Cifrado	Estado de cifrado del servidor de origen de datos.
Supervisión	Estado del agente de supervisión.
Ubicación geográfica	Ubicación geográfica del origen de datos.

El origen de datos que ha añadido aparece en la lista en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Servidor**.

Crear y activar una exploración de evaluación de puntos finales

Utilice el componente Evaluación de vulnerabilidades de IBM Data Risk Manager para crear y ejecutar la exploración de evaluación en IBM QRadar Security Intelligence Platform para identificar las vulnerabilidades de punto final.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM QRadar Security Intelligence Platform. Para obtener más información sobre la integración, consulte "Integración de IBM QRadar Security Intelligence Platform con IBM Data Risk Manager" en la página 54.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación ⁞⁞⁞.
3. Pulse **Gestión de vulnerabilidades**.
4. Seleccione un programa de la lista.
5. Pulse **Crear nueva evaluación**.
6. En la página **Crear nueva evaluación**, establezca las opciones siguientes y pulse **Crear evaluación**.

Opción	Descripción
Nombre de evaluación	Nombre de la evaluación de puntos finales de IBM QRadar Security Intelligence Platform.
Tipo de exploración	El tipo de exploración, por ejemplo, `Explorador de vulnerabilidades del servidor`.
Ejecutar el	Instancia del adaptador de IBM QRadar Security Intelligence Platform para ejecutar el proceso de evaluación de vulnerabilidades.

7. En **Ámbito de evaluación**, añada orígenes de datos a la transacción en función del ámbito o de los últimos días de exploración. Puede añadir varios orígenes de datos.
8. Pulse **Añadir ámbito a transacción**.
9. En **Transacciones pendientes** en la vista Transacción, pulse el icono **Iniciar proceso**  .
10. Seleccione **Explorar ahora**.

    Para planificar la exploración más tarde, seleccione **Explorar después**.

    Para guardar los detalles de la transacción tras la finalización del proceso en **Transacciones pendientes** para su reutilización, seleccione **Réplica**.
11. Para ejecutar el proceso, pulse el icono **Activar evaluación**  .

Ver el estado de la exploración

Utilice el componente Centro de control y mandatos de seguridad (SC3) de IBM Data Risk Manager para ver el estado de la exploración y realizar un análisis y acciones adicionales.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú  .
3. Seleccione un programa de la lista.
4. Vaya a **Centro de control y mandatos de seguridad** > **Inicio**.
5. Para ver la lista de procesos completados junto con el estado, pulse **Procesos de evaluación de vulnerabilidad**.

Ver resultados de la exploración de evaluación de puntos finales de IBM QRadar Security Intelligence Platform

Utilice el componente Evaluación de vulnerabilidades de IBM Data Risk Manager para ver los resultados de la exploración de evaluación de puntos finales para realizar un análisis y acciones adicionales.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Pulse **Gestión de vulnerabilidades**.
4. Pulse **Ver resultados**.
5. Pulse el icono Filtro  en **Orígenes de datos VA** y seleccione el tipo de adaptador, por ejemplo, `IBM QRadar`.
6. Para la evaluación seleccionada, pulse el número para **Aprobado**, **Error** u **Otros** para visualizar los resultados en la página **Resultados de prueba de vulnerabilidades**.

Importación de exploración de vulnerabilidades desde IBM QRadar Security Intelligence Platform
Puede importar exploraciones de vulnerabilidad desde dispositivos IBM QRadar Security Intelligence Platform en el inventario de IBM Data Risk Manager para el análisis de riesgos.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con IBM QRadar Security Intelligence Platform. Para obtener más información sobre la integración, consulte "Integración de IBM QRadar Security Intelligence Platform con IBM Data Risk Manager" en la página 54.

Cuando se desencadena la exploración VA desde IBM Data Risk Manager, si dicha exploración falla en IBM Data Risk Manager y termina en IBM QRadar Security Intelligence Platform, no se podrá importar, ya que no hay ningún concepto de origen de datos en IBM QRadar Security Intelligence Platform. IBM QRadar Security Intelligence Platform tiene el concepto de Activo, que tiene la dirección IP del punto final.

Acerca de esta tarea

El icono de transacción  indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción  indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Exploraciones de datos**.
4. Importe las exploraciones de datos.
   a) Pulse el icono **Descargar**  .
   b) En la ventana **Importar**, seleccione **Evaluación de vulnerabilidad**.
   c) Desde la lista **Adaptador**, seleccione **IBM QRadar**.
   d) En la lista **Instancias**, seleccione una instancia de adaptador. Puede seleccionar hasta tres instancias.
   e) Pulse **Importar**. Cuando la operación de importación se haya completado, las exploraciones de IBM QRadar Security Intelligence Platform se añaden al inventario.
   f) Para renovar la lista de inventario de exploraciones de datos, pulse el icono **Renovar**  .
5. Para ver los resultados después de la operación de importación, vaya a **Centro de control y mandatos de seguridad** > **Inicio**.

Importar vulnerabilidades como un archivo CSV a IBM Data Risk Manager
Utilice el componente Modelador de contexto empresarial de IBM Data Risk Manager para importar las vulnerabilidades como un archivo CSV a IBM Data Risk Manager.

Antes de empezar

Asegúrese de que los datos de contexto empresarial estén disponibles para importarlos.

Puede descargar las plantillas de ejemplo en: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**.
4. Habilite el botón de conmutación **Datos de catálogo**.
5. Seleccione **Vulnerabilidad**.
6. Pulse **Elegir archivo** para localizar y seleccionar el archivo.
7. Pulse **Cargar**.

   Los datos se visualizan para su verificación.
8. Pulse **Importar**.

Creación de una actividad para reparar vulnerabilidades

Utilice el componente Gestión de vulnerabilidades de IBM Data Risk Manager para ver y reparar vulnerabilidades. Cuando se identifican las vulnerabilidades mediante exploraciones, se deben llevar a cabo acciones de reparación para evaluar la exposición de riesgo correcta para el activo de información.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Pulse **Gestión de vulnerabilidades**.
4. Vaya a **Vista de resultados**.
5. Pulse **Orígenes de datos VA**.
6. Pulse el icono de filtro en **Orígenes de datos VA** y seleccione el tipo de adaptador, por ejemplo, `IBM QRadar`.
7. De forma alternativa, puede seleccionar un origen de datos basado en la plataforma.
   a) Pulse **Plataformas VA**.
   b) Seleccione una plataforma y pulse el icono de base de datos  para seleccionar el origen de datos.
8. Para un origen de datos seleccionado, pulse el número para **Error** para mostrar los resultados en la página **Resultados de la prueba de vulnerabilidades**.
9. Pulse el icono de flecha hacia abajo  para seleccionar el nivel de gravedad.
10. Pulse el icono **Reparación** .
11. Pulse **Sí** para crear acciones de reparación.
12. En la ventana **Crear actividad de reparación**, especifique la información necesaria. Si el origen de datos procede de ServiceNow, puede publicar la actividad como incidencia en ServiceNow para la gestión de reparaciones.
13. Pulse **Crear**.

    En la página **Resultados de la prueba de vulnerabilidades**, en **Actividad**, puede ver los detalles de actividad si la fecha de finalización de la actividad es mayor que la fecha de ejecución de los resultados de prueba.

Qué hacer a continuación

Puede ver y gestionar las actividades de reparación que ha definido en las áreas siguientes.

Centro de acción de IBM Data Risk Manager

- Pulse el icono de menú de aplicación .
- Pulse **Centro de acción**.

Para obtener más información sobre el Centro de acción, consulte "Centro de acción" en la página 151.

La ventana Detalles de activo en el panel de control de IBM Data Risk Manager

- Pulse el icono de menú de aplicación .
- Pulse **Panel de control**.
- En la ventana **Conjunto de activos de información**, pulse el icono de flecha en el activo para ver los detalles del activo.
- En la ventana **Detalles de activo**, pulse **Infraestructura** > **Vulnerabilidades**.
- Para ver elementos de acción, seleccione el nodo de infraestructura y pulse **Elementos de acción**.

Integración de IBM Security AppScan Enterprise con IBM Data Risk Manager

Las vulnerabilidades de aplicación para las aplicaciones exploradas en IBM Security AppScan Enterprise se pueden importar a IBM Data Risk Manager. IBM Data Risk Manager puede desencadenar la exploración de evaluación de vulnerabilidades.

El agente de Intercambio de integración de IBM Data Risk Manager (IntEx) se utiliza para consumir vulnerabilidades de aplicaciones de IBM Security AppScan Enterprise.

Para obtener más información sobre los requisitos previos de instalación, consulte "Requisitos previos de instalación" en la página 18.

La importación de las vulnerabilidades de aplicaciones desde IBM Security AppScan Enterprise y la activación de la exploración de evaluación de vulnerabilidades en IBM Data Risk Manager incluye las siguientes tareas:

- Integración de IBM Security AppScan Enterprise con IBM Data Risk Manager.
- Importar plantillas de exploración de IBM Security AppScan Enterprise.
- Creación del inventario de aplicaciones en IBM Data Risk Manager.
- Importar datos de contexto.
- Crear evaluación de aplicaciones.
- Ver el estado de la exploración de evaluación de aplicaciones.
- Ver el resultado de la exploración de evaluación de aplicaciones.
- Correlacionar la vulnerabilidad en el panel de control de IBM Data Risk Manager.
- Importar vulnerabilidades de IBM Security AppScan Enterprise a IBM Data Risk Manager.
- Importar vulnerabilidades de puntos finales como un archivo CSV a IBM Data Risk Manager.

Integración de IBM Security AppScan Enterprise con IBM Data Risk Manager

Configure IBM Data Risk Manager para que se comunique con IBM Security AppScan Enterprise. Para obtener información sobre los pasos de configuración, consulte "Integración de IBM Security AppScan Enterprise con IBM Data Risk Manager" en la página 62.

Importar plantillas de exploración de IBM Security AppScan Enterprise

Importe las plantillas de exploración de IBM Security AppScan Enterprise a IBM Data Risk Manager. Para ver los pasos para importar plantillas, consulte "Importar la plantilla de exploración de IBM Security AppScan Enterprise a IBM Data Risk Manager" en la página 63.

Creación del inventario de aplicaciones en IBM Data Risk Manager

Añada los orígenes de datos de IBM Security AppScan Enterprise a IBM Data Risk Manager. Para ver los pasos sobre cómo añadir orígenes de datos, consulte "Adición de orígenes de datos de IBM Security AppScan Enterprise" en la página 63.

Importar datos de contexto

Importe datos de contexto. Asegúrese de que los datos de contexto se guarden correctamente y que los atributos se correlacionen correctamente con el inventario adecuado que se ha creado anteriormente. Para obtener más información sobre cómo importar los datos de contexto, consulte "Correlación de datos de contexto empresarial" en la página 106.

Nota: Se puede crear el inventario en IBM Data Risk Manager proporcionando el nombre del origen de datos y el tipo en la hoja de datos de contexto `Base de datos`.

Crear evaluación de aplicaciones

Utilice el componente Evaluación de vulnerabilidades de IBM Data Risk Manager para crear la evaluación de aplicaciones. Para ver los pasos sobre cómo crear la evaluación de aplicaciones, consulte "Crear y activar una evaluación de aplicaciones" en la página 64.

Ver el estado de la exploración de evaluación de aplicaciones

Puede ver el estado de la exploración de evaluación de aplicaciones para continuar con un análisis y acciones adicionales. Para ver los pasos sobre cómo ver el estado de la exploración, consulte Ver estado de la exploración.

Ver el resultado de la exploración de evaluación de aplicaciones

Vea los resultados de la exploración de evaluación de aplicaciones para realizar un análisis y acciones adicionales. Para ver los pasos sobre cómo ver los resultados de la exploración, consulte Ver estado de la exploración.

Correlacionar la vulnerabilidad en el panel de control de IBM Data Risk Manager

Cuando se ha completado correctamente la exploración de la evaluación de aplicaciones, puede ver el recuento de vulnerabilidades de aplicaciones en el widget Aplicación del panel de control de IBM Data Risk Manager. Para obtener más información sobre el panel de control, consulte "Panel de control de IBM Data Risk Manager" en la página 177

Nota: El recuento visualizado es el recuento de vulnerabilidades agregadas, incluido el recuento de la infraestructura relacionada.

Importar vulnerabilidades de IBM Security AppScan Enterprise a IBM Data Risk Manager

Importe las exploraciones de vulnerabilidades desde los dispositivos de IBM Security AppScan Enterprise al inventario de IBM Data Risk Manager para clasificar los datos y analizar riesgos. Para ver los pasos sobre cómo importar la exploración, consulte Importar exploraciones de vulnerabilidades.

Nota: Cuando importa las exploraciones, también se importan los orígenes de datos y los resultados de las importaciones.

Importar vulnerabilidades de aplicaciones como un archivo CSV a IBM Data Risk Manager

Puede importar vulnerabilidades de aplicaciones como un archivo CSV a IBM Data Risk Manager. Para ver los pasos sobre cómo importar el archivo CSV, consulte Importar exploraciones de vulnerabilidades.

Reparación de vulnerabilidades

Cuando se identifican las vulnerabilidades mediante exploraciones, se deben llevar a cabo acciones de reparación para evaluar la exposición de riesgo correcta para el activo de información. Para ver los pasos

sobre cómo definir acciones de reparación, consulte “Creación de una actividad para reparar vulnerabilidades ” en la página 48.

Integración de IBM Security AppScan Enterprise con IBM Data Risk Manager
Puede configurar IBM Data Risk Manager para que se comunique con IBM Security AppScan Enterprise y utilizar la información de riesgo confidencial en IBM Data Risk Manager para las evaluaciones.

Acerca de esta tarea

El componente Modelador de contexto empresarial (BCM) de IBM Data Risk Manager proporciona el Asistente de integración de empresa para integrar IBM Security AppScan Enterprise con IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
4. En la sección Configuración del adaptador, pulse el icono **Añadir adaptador de integración** .
5. Seleccione **IBM AppScan** en la lista.
6. Para añadir una instancia de IBM Security AppScan Enterprise, seleccione **IBM AppScan** en la lista de Configuración de adaptador.
7. En la sección Instancias de integración, pulse el icono **Añadir instancia** .
8. Establezca las siguientes opciones.

Opción	Descripción
Nombre	Especifique un nombre para la instancia de IBM Security AppScan Enterprise.
URL	Especifique el URL para acceder a IBM Security AppScan Enterprise, por ejemplo, `https://<IP-aplicación appscan/nombre de host:puerto>`.
Instancia de microservicio	Seleccione el agente necesario para la integración.
Nombre de usuario	Especifique el nombre de usuario de IBM Security AppScan Enterprise con el rol de administrador.
Contraseña	Especifique la contraseña para el nombre de usuario.
Clave de característica de AppScan	Especifique la clave para establecer conexión con IBM Security AppScan Enterprise.
Clasificador y evaluación de vulnerabilidades	Especifique el archivo de configuración para importar datos del servidor de integración a IBM Data Risk Manager para las evaluaciones de vulnerabilidad y clasificación de datos.

9. Pulse **Guardar** para guardar los detalles de configuración.

Qué hacer a continuación
Para la instancia de adaptador que ha creado, puede probar la conectividad. Seleccione la instancia en la lista de **Instancias de integración** y, a continuación, pulse **Probar conexión** para probar si la comunicación entre la instancia de IBM Security AppScan Enterprise y el servidor IBM Data Risk Manager es satisfactoria.

Importar la plantilla de exploración de IBM Security AppScan Enterprise a IBM Data Risk Manager
Importe la plantilla de exploración de IBM Security AppScan Enterprise a IBM Data Risk Manager para analizar y evaluar los datos.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Pruebas VA**.
4. Para descargar plantillas de exploración, pulse el icono **Descargar** .
5. En la ventana **Importar**, seleccione una instancia de adaptador para IBM Security AppScan Enterprise.
6. Pulse **Importar**. Cuando la operación de importación se haya completado, las pruebas VA se añaden al inventario.
7. Para renovar la lista de inventario de pruebas VA, pulse el icono **Renovar** .

Adición de orígenes de datos de IBM Security AppScan Enterprise
Puede añadir orígenes de datos de IBM Security AppScan Enterprise en el inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con IBM Security AppScan Enterprise. Para obtener más información sobre la integración, consulte "Integración de IBM Security AppScan Enterprise con IBM Data Risk Manager" en la página 62.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.
4. Para añadir un origen de datos de IBM Security AppScan Enterprise, pulse el icono **Añadir origen de datos** .
5. En la página **Añadir origen de datos**, establezca las opciones siguientes y pulse **Añadir**.

Opción	Descripción
Tipo de servidor	El tipo de servidor que desea utilizar. Por ejemplo, **IBM Appscan**.
Nombre de origen de datos	Nombre exclusivo para el origen de datos.
URL de host	El URL del servidor de host para importar datos.
Dirección IP	Dirección IP del servidor.
Puerto	Número de puerto para conectarse al servidor.
Adaptador	Nombre de instancia de IBM Security AppScan Enterprise. Por ejemplo, `AppScan_Instance`.
Agentes	El nombre de agente para conectarse al servidor.

Opción	Descripción
Nombre de usuario	El nombre del usuario para conectarse al servidor.
Contraseña	Contraseña para el nombre de usuario.
Cifrado	Estado de cifrado del servidor de origen de datos.
Supervisión	Estado del agente de supervisión.
Ubicación geográfica	Ubicación geográfica del origen de datos.

El origen de datos que ha añadido aparece listado en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Aplicación**.

Crear y activar una evaluación de aplicaciones

Utilice el componente Gestión de vulnerabilidades de IBM Data Risk Manager para crear y ejecutar la exploración de evaluación en IBM Security AppScan Enterprise para identificar las vulnerabilidades de aplicaciones.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security AppScan Enterprise. Para obtener información sobre la integración, consulte "Integración de IBM Security AppScan Enterprise con IBM Data Risk Manager" en la página 62.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Pulse **Gestión de vulnerabilidades**.
4. Seleccione un programa de la lista.
5. Pulse **Crear nueva evaluación**.
6. En la página **Crear nueva evaluación**, establezca las opciones siguientes y pulse **Crear evaluación**.

Opción	Descripción
Nombre de evaluación	Nombre de la evaluación de aplicaciones de IBM Security AppScan Enterprise.
Tipo de exploración	El tipo de exploración, por ejemplo, `Explorador de aplicaciones`.
Ejecutar el	Instancia del adaptador de IBM Security AppScan Enterprise donde se ejecutará el proceso de evaluación.

7. En **Ámbito de evaluación**, añada orígenes de datos a la transacción en función del ámbito o de los últimos días de exploración. Solo se puede añadir un origen de datos al ámbito de la transacción.
8. Pulse **Añadir ámbito a transacción**.
9. Seleccione la prueba de vulnerabilidad en la lista y pulse **Guardar**.
10. En **Transacciones pendientes** en la vista Transacción, pulse el icono **Iniciar proceso**  .
11. Seleccione **Explorar ahora**.

    Para planificar la exploración más tarde, seleccione **Explorar después** y especifique la hora a la que se debe ejecutar la exploración.

Para guardar los detalles de la transacción tras la finalización del proceso en **Transacciones pendientes** para su reutilización, seleccione **Réplica**.

12. Para iniciar el proceso, pulse el icono **Activar evaluación** .

Ver el estado de la exploración
Utilice el componente Centro de control y mandatos de seguridad (SC3) de IBM Data Risk Manager para ver el estado de la exploración y realizar un análisis y acciones adicionales.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú .
3. Seleccione un programa de la lista.
4. Vaya a **Centro de control y mandatos de seguridad** > **Inicio**.
5. Para ver la lista de procesos completados junto con el estado, pulse **Procesos de evaluación de vulnerabilidad**.

Ver los resultados de la exploración de evaluación de aplicaciones de IBM Security AppScan Enterprise
Utilice el componente Evaluación de vulnerabilidades de IBM Data Risk Manager para ver los resultados de la exploración de evaluación de aplicaciones para realizar un análisis y acciones adicionales.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Pulse **Gestión de vulnerabilidades**.
4. Pulse **Ver resultados**.
5. Pulse el icono Filtro en **Orígenes de datos VA** y seleccione el tipo de adaptador, por ejemplo, IBM AppScan.
6. Para la evaluación seleccionada, pulse el número para **Aprobado**, **Error** u **Otros** para visualizar los resultados en la página **Resultados de prueba de vulnerabilidades**.

Importación de exploraciones de evaluación de vulnerabilidades desde IBM Security AppScan Enterprise
Puede importar exploraciones de evaluación de vulnerabilidades desde dispositivos IBM Security AppScan Enterprise al inventario de IBM Data Risk Manager para el análisis de riesgos.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con IBM Security AppScan Enterprise. Para obtener más información sobre los pasos de integración, consulte "Integración de IBM Security AppScan Enterprise con IBM Data Risk Manager" en la página 62.

Acerca de esta tarea

El icono de transacción indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Exploraciones de datos**.
4. Importe las exploraciones de datos.
   a) Pulse el icono **Descargar** .
   b) En la ventana **Importar**, seleccione **Evaluación de vulnerabilidad**.
   c) Desde la lista **Adaptador**, seleccione **IBM AppScan**.
   d) En la lista **Instancias**, seleccione una instancia de adaptador. Puede seleccionar hasta tres instancias.
   e) Pulse **Importar**. Cuando se haya completado la operación de importación, las exploraciones de evaluación de vulnerabilidades de IBM Security AppScan Enterprise se añaden al inventario.
   f) Para renovar la lista de inventario de exploraciones de datos, pulse el icono **Renovar** .
5. Para ver los resultados de la exploración después de la operación de importación, vaya a **Centro de control y mandatos de seguridad** > **Inicio**.

Importar vulnerabilidades como un archivo CSV a IBM Data Risk Manager
Utilice el componente Modelador de contexto empresarial de IBM Data Risk Manager para importar las vulnerabilidades como un archivo CSV a IBM Data Risk Manager.

Antes de empezar

Asegúrese de que los datos de contexto empresarial estén disponibles para importarlos.

Puede descargar las plantillas de ejemplo en: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**.
4. Habilite el botón de conmutación **Datos de catálogo**.
5. Seleccione **Vulnerabilidad**.
6. Pulse **Elegir archivo** para localizar y seleccionar el archivo.
7. Pulse **Cargar**.
   Los datos se visualizan para su verificación.
8. Pulse **Importar**.

Creación de una actividad para reparar vulnerabilidades
Utilice el componente Gestión de vulnerabilidades de IBM Data Risk Manager para ver y reparar vulnerabilidades. Cuando se identifican las vulnerabilidades mediante exploraciones, se deben llevar a cabo acciones de reparación para evaluar la exposición de riesgo correcta para el activo de información.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Pulse **Gestión de vulnerabilidades**.
4. Vaya a **Vista de resultados**.
5. Pulse **Orígenes de datos VA**.
6. Pulse el icono de filtro en **Orígenes de datos VA** y seleccione el tipo de adaptador, por ejemplo, `IBM QRadar`.
7. De forma alternativa, puede seleccionar un origen de datos basado en la plataforma.
   a) Pulse **Plataformas VA**.
   b) Seleccione una plataforma y pulse el icono de base de datos  para seleccionar el origen de datos.
8. Para un origen de datos seleccionado, pulse el número para **Error** para mostrar los resultados en la página **Resultados de la prueba de vulnerabilidades**.
9. Pulse el icono de flecha hacia abajo  para seleccionar el nivel de gravedad.
10. Pulse el icono **Reparación** .
11. Pulse **Sí** para crear acciones de reparación.
12. En la ventana **Crear actividad de reparación**, especifique la información necesaria. Si el origen de datos procede de ServiceNow, puede publicar la actividad como incidencia en ServiceNow para la gestión de reparaciones.
13. Pulse **Crear**.

    En la página **Resultados de la prueba de vulnerabilidades**, en **Actividad**, puede ver los detalles de actividad si la fecha de finalización de la actividad es mayor que la fecha de ejecución de los resultados de prueba.

Qué hacer a continuación

Puede ver y gestionar las actividades de reparación que ha definido en las áreas siguientes.

Centro de acción de IBM Data Risk Manager

- Pulse el icono de menú de aplicación .
- Pulse **Centro de acción**.

Para obtener más información sobre el Centro de acción, consulte "Centro de acción" en la página 151.

La ventana Detalles de activo en el panel de control de IBM Data Risk Manager

- Pulse el icono de menú de aplicación .
- Pulse **Panel de control**.
- En la ventana **Conjunto de activos de información**, pulse el icono de flecha en el activo para ver los detalles del activo.
- En la ventana **Detalles de activo**, pulse **Infraestructura** > **Vulnerabilidades**.
- Para ver elementos de acción, seleccione el nodo de infraestructura y pulse **Elementos de acción**.

Integración de DLP de Symantec con IBM Data Risk Manager

Puede importar las incidencias no estructuradas marcadas como falsos positivos en DLP de Symantec a IBM Data Risk Manager. A continuación, se correlacionan los datos con la infraestructura adecuada en IBM Data Risk Manager.

IBM Data Risk Manager utiliza el siguiente microservicio para utilizar incidencias no estructuradas desde DLP de Symantec que se ejecuta en el puerto 8764.

```
Agente Symantec
```

Para obtener más información sobre los requisitos previos de instalación, consulte "Requisitos previos de instalación" en la página 18.

Asegúrese de que tiene la imagen de IBM Data Risk Manager Server o que el build está disponible en el formato necesario, en función del entorno en el que está ejecutando la instalación.

Para importar incidencias no estructuradas desde DLP de Symantec, ejecute las tareas siguientes.

- Integración de IBM Data Risk Manager con DLP de Symantec – enlace directo.
  - Creación de incidencias en DLP de Symantec.
    - Descubrimiento de datos confidenciales.
    - Protección de datos confidenciales.
  - Integración de DLP de Symantec con IBM Data Risk Manager.
  - Importar incidencias a IBM Data Risk Manager.
  - Importar datos de contexto.
  - Correlación de incidencias con la infraestructura en el panel de control de IBM Data Risk Manager.
  - Importar políticas de DLP de Symantec a IBM Data Risk Manager.
- Integración de IBM Data Risk Manager con DLP de Symantec – Importar incidencias mediante un archivo CSV.
  - Creación de DLP de Symantec - Inventario no estructurado en IBM Data Risk Manager.
  - Importar incidencias DLP de Symantec como un archivo CSV a IBM Data Risk Manager
  - Importar datos de contexto.
  - Correlación de incidencias con la infraestructura en el panel de control de IBM Data Risk Manager.

Descubrimiento de datos confidenciales

Identifique los datos confidenciales (archivos) que se encuentran en una ubicación específica del servidor de Windows. Asegúrese de que tiene una compartición SMB en dicha carpeta.

Protección de datos confidenciales

1. Cree las políticas.
   a. Cree un grupo de políticas.
   b. Cree una o varias políticas y asígnelas a un grupo de políticas.
2. Cree los destinos.
   a. Cuando cree un destino en pestaña **contenido explorado**, añada la raíz del contenido con la ubicación de la carpeta completa.
   b. Seleccione varios grupos de políticas o un grupo de políticas único.
3. Active la exploración de DLP de Symantec en el destino para generar una incidencia (violación producida en un archivo basada en la política).
4. Capture los resultados de la incidencia y guárdelos como un informe que se utilizará para una resolución adicional. Anote el ID de informe que se muestra en el URL.

Cuando se guardan las incidencias como un informe con un nombre diferente, se genera el ID de informe adecuado y se muestra en el URL. Utilice el ID de informe para el registro en DLP de Symantec. Puede exportar estas incidencias como un archivo CSV.

5. Personalice el informe, según sea necesario, basado en factores como un destino específico para el que se necesita el informe, la exploración que se ejecuta en una fecha específica o el filtro de gravedad.

Integración de DLP de Symantec con IBM Data Risk Manager

Para ver los pasos de integración, consulte "Integración de Symantec DLP con IBM Data Risk Manager" en la página 69.

Importar incidencias a IBM Data Risk Manager

Para ver los pasos sobre cómo importar incidencias, consulte "Importar incidencias desde DLP de Symantec" en la página 70.

Importar políticas de DLP de Symantec a IBM Data Risk Manager.

Para ver los pasos sobre cómo importar políticas, consulte "Importar políticas de DLP de Symantec a IBM Data Risk Manager" en la página 71.

Creación de DLP de Symantec - Inventario no estructurado en IBM Data Risk Manager

Para ver los pasos para crear un inventario no estructurado, consulte "Adición de orígenes de datos de DLP de Symantec" en la página 71.

Importar incidencias de DLP de Symantec como un archivo CSV a IBM Data Risk Manager

Para ver los pasos para importar incidencias como un archivo CSV, consulte "Importar incidencias de DLP de Symantec como un archivo CSV a IBM Data Risk Manager" en la página 72.

Importar datos de contexto

Importe datos de contexto. Asegúrese de que los datos de contexto se guarden correctamente y que los atributos se correlacionen correctamente con el inventario adecuado que se ha creado anteriormente. Para obtener más información sobre cómo importar los datos de contexto, consulte "Correlación de datos de contexto empresarial" en la página 106.

Nota: Se puede crear el inventario en IBM Data Risk Manager proporcionando el nombre del origen de datos y el tipo en la hoja de datos de contexto `Base de datos`.

Correlación de incidencias con la infraestructura en el panel de control de IBM Data Risk Manager

1. Cuando las exploraciones o el archivo CSV de DLP de Symantec se importan correctamente, las políticas asociadas al destino están disponibles en **Activo recién descubierto** bajo la sección **No estructurado** de la página Taxonomía.
2. Aplique los atributos de taxonomía y exporte los activos no estructurados al panel de control.

   Nota: En los atributos de Taxonomía, `Aplicación` no es aplicable a `Activo no estructurado`.

Integración de Symantec DLP con IBM Data Risk Manager

Puede configurar IBM Data Risk Manager para que se comunique con Symantec DLP (Data Loss Prevention connection) para importar incidencias y políticas de DLP de Symantec en IBM Data Risk Manager.

Acerca de esta tarea

El componente Modelador de contexto empresarial (BCM) de IBM Data Risk Manager proporciona el Asistente de integración de empresa para integrar DLP de Symantec con IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
4. En la sección Configuración del adaptador, pulse el icono **Añadir adaptador de integración** .
5. Seleccione **DLP de Symantec** en la lista.
6. Para añadir una instancia de DLP de Symantec, seleccione **DLP de Symantec** en la lista de Configuración de adaptador.
7. En la sección Instancias de integración, pulse el icono **Añadir instancia** .
8. Establezca las siguientes opciones.

Opción	Descripción
Nombre	Especifique un nombre para la instancia de DLP de Symantec.
URL	Especifique el URL para acceder a DLP de Symantec, por ejemplo, `https://<IP-aplicación symantec/nombre de host:puerto>`.
Instancia de microservicio	Seleccione la instancia de microservicio necesaria para la integración.
Versión de Symantec DLP	Seleccione una versión de DLP de Symantec para importar incidencias y políticas.
Nombre de usuario	Especifique el nombre de usuario de DLP de Symantec con el rol de administrador.
Contraseña	Especifique la contraseña para el nombre de usuario.
Guardar ID de informes (separados por comas)	Especifique una lista separada por comas de los ID de informe guardados para importar los informes de incidencias correspondientes.

9. Pulse **Guardar** para guardar los detalles de configuración.

Qué hacer a continuación

Para la instancia de adaptador que ha creado, puede probar la conectividad. Seleccione la instancia en la lista de **Instancias de integración** y, a continuación, pulse **Probar conexión** para probar si la comunicación entre la instancia de DLP de Symantec y el servidor IBM Data Risk Manager es satisfactoria.

Importar incidencias desde DLP de Symantec

Puede importar incidencias desde DLP de Symantec al inventario de IBM Data Risk Manager para clasificar datos y analizar riesgos.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con DLP de Symantec. Para obtener más información sobre los pasos de integración, consulte “Integración de Symantec DLP con IBM Data Risk Manager” en la página 69.

Acerca de esta tarea

El icono de transacción indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Exploraciones de datos**.
4. Importe las exploraciones de datos.
   a) Pulse el icono **Descargar** .
   b) Desde la lista **Adaptador**, seleccione **DLP de Symantec**.
   c) En la lista **Instancias**, seleccione una instancia de adaptador.
   d) Pulse **Importar** para importar las exploraciones.
   e) Para renovar la lista de inventario de exploraciones, pulse el icono **Renovar** .
5. Para ver los resultados de la exploración después de la operación de importación, vaya a **Centro de control y mandatos de seguridad** > **Inicio**.

Importar políticas de DLP de Symantec a IBM Data Risk Manager

Puede importar políticas de DLP de Symantec en el inventario de IBM Data Risk Manager para la clasificación de datos y el análisis de riesgos.

Acerca de esta tarea

El icono de transacción indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Políticas**.
4. Importar políticas.
   a) Pulse el icono **Descargar** .
   b) En la ventana **Importar**, seleccione una instancia de DLP de Symantec en la lista de **Instancias**.
   c) Pulse **Seleccionar archivos** para seleccionar el archivo XML.

      Nota: En DLP de Symantec, exporte las políticas a un archivo XML.

      Cuando se hayan cargado correctamente las políticas, podrá ver las políticas en **Gestión de políticas** > **Limpieza de políticas** > **Sin estructurar**. Puede utilizar estas políticas para activar la exploración nativa no estructurada.

Adición de orígenes de datos de DLP de Symantec

Puede añadir orígenes de datos DLP de Symantec en el inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con DLP de Symantec. Para obtener más información sobre la integración, consulte "Integración de Symantec DLP con IBM Data Risk Manager" en la página 69.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.
4. Para añadir un origen de datos de DLP de Symantec, pulse el icono **Añadir origen de datos**  .
5. En la página **Añadir origen de datos**, establezca las opciones siguientes y pulse **Añadir**.

Opción	Descripción
Tipo de servidor	El tipo de servidor de origen de datos que desea utilizar. Por ejemplo, **IDRM**.
Destino	Nombre del origen de datos.
Dirección IP	La dirección IP del servidor de origen de datos.
Puerto	Número de puerto para conectarse al servidor.
Tipo de puerto	El protocolo de compartición de archivos par acceder a datos.
Vía de acceso de destino	Vía de acceso de destino para importar los datos no estructurados.
Adaptador	Nombre de instancia de DLP de Symantec. Por ejemplo, `Instancia de DLP de Symantec`.
Agentes	Nombre de agente para conectarse al origen de datos.
Nombre de usuario	Nombre del usuario.
Contraseña	Contraseña para el nombre de usuario.
Cifrado	Estado de cifrado del servidor de origen de datos.
Supervisión	Estado del servidor de origen de datos de agente de supervisión.
Ubicación geográfica	Ubicación geográfica del origen de datos.

El origen de datos que ha añadido se muestra en la lista en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Almacenamiento de archivos**.

Importar incidencias de DLP de Symantec como un archivo CSV a IBM Data Risk Manager
Puede importar incidencias de DLP de Symantec al inventario de IBM Data Risk Manager para clasificación de datos y análisis de riesgos.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .

3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**.
4. Habilite el botón de conmutación **Datos de catálogo**.
5. Pulse la pestaña **Incidencias**.
6. Pulse **Elegir archivo** para localizar y seleccionar el archivo.
7. Pulse **Cargar**.
   Los datos se visualizan para su verificación.
8. Pulse **Importar**.

   Nota: Asegúrese de que se ha creado el inventario en IBM Data Risk Manager antes de cargar el archivo CSV.

Integración de ServiceNow con IBM Data Risk Manager

Debe configurar ServiceNow para importar los datos de CMDB (Base de datos de gestión de configuración) a IBM Data Risk Manager y utilizar estos datos junto con las aplicaciones y el contexto empresarial. También puede publicar las actividades que se crean en el Centro de acción para ServiceNow para las actividades de reparación.

una actividad y publicarla como una incidencia en ServiceNow para la gestión de reparaciones.

IBM Data Risk Manager utiliza el siguiente microservicio para utilizar las vulnerabilidades de las aplicaciones desde ServiceNow que se ejecuta en el puerto 8787.

```
ServiceNow (Consumo de datos CMDB) – se ejecuta en el puerto 8787
```

Para obtener más información sobre los requisitos previos, consulte “Requisitos previos de instalación” en la página 18.

Asegúrese de que tiene la imagen de IBM Data Risk Manager Server o que el build está disponible en el formato necesario, en función del entorno en el que está ejecutando la instalación.

Para importar los datos CMDB ServiceNow a IBM Data Risk Manager, ejecute las tareas siguientes.

- Integración de ServiceNow con IBM Data Risk Manager.
- Importar datos CMDB de ServiceNow a IBM Data Risk Manager.
- Correlación de la entidad ServiceNow con IBM Data Risk Manager

Integración de ServiceNow con IBM Data Risk Manager

Para ver los pasos de integración, consulte “Integración de ServiceNow con IBM Data Risk Manager” en la página 74.

Importar datos CMDB de ServiceNow a IBM Data Risk Manager

Para ver los pasos de importación, consulte “Importar CMDB de ServiceNow a IBM Data Risk Manager” en la página 75.

Correlación de la entidad ServiceNow con IBM Data Risk Manager

Debe utilizar el modo de autenticación básico para conectar con ServiceNow. La tabla siguiente ilustra la correlación de claves entre las entidades de ServiceNow e IBM Data Risk Manager.

Entidad ServiceNow	Entidad de correlación
cmdb_ci_business_app	Aplicación
cmdb_ci_service	Aplicación
cmdb_ci_appl	Aplicación
cmdb_ci_business_process	Proceso empresarial

cmdb_ci_database	Inventario
cmdb_ci_app_server	Inventario
cmdb_ci_db_instance	Inventario
cmdb_ci_server	Inventario
cmdb_ci_ip_address	Se utiliza de forma interna para correlacionar la dirección IP del inventario utilizando el objeto `cmdb_rel_ci`.
cmn_department	Se utiliza para resolver la lista de valores de departamentos.
cmdb_rel_ci	Objeto de relación de entidades que se utiliza para establecer la relación entre entidades.
cmn_cost_center	Se utiliza para resolver la lista de valores de departamentos
cmdb_rel_type	Lista maestra de tipo de relación
sys_user	Lista maestra de recursos y usuario
cmn_location	Se utiliza para resolver la lista de valores de ubicación
core_company	Se utiliza para resolver la lista de valores de empresa

Cuando se importan los datos CMDB a IBM Data Risk Manager, en función de la correlación de entidad, automáticamente se lleva a cabo la resolución de datos de contexto y el etiquetado. Ahora los inventarios cuyo origen es ServiceNow se pueden gestionar correctamente, (Base de datos, Almacenamiento de archivos, Aplicación y Servidor)en **Modelador de contexto empresarial** > **Gestionar inventario**.

Publicación de actividades en ServiceNow para la gestión de reparaciones

Para un origen de datos ServiceNow, puede crear una actividad en el Centro de acción y publicarlo como una incidencia en ServiceNow para la gestión de reparaciones. Actualmente, puede publicar la actividad solo en una única instancia de ServiceNow. Para obtener más información sobre el Centro de acción, consulte “Centro de acción” en la página 151.

Integración de ServiceNow con IBM Data Risk Manager

Debe configurar IBM Data Risk Manager para que se conecte e interactúe con ServiceNow para importar los datos de CMDB (Base de datos de gestión de configuración) a IBM Data Risk Manager y utilizar estos datos junto con las aplicaciones y el contexto empresarial.

Acerca de esta tarea

El componente Modelador de contexto empresarial (BCM) de IBM Data Risk Manager proporciona el Asistente de integración de empresa para integrar ServiceNow con IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
4. En la sección Configuración del adaptador, pulse el icono **Añadir adaptador de integración** .
5. Seleccione **ServiceNow** en la lista.
6. Para añadir una instancia de ServiceNow, seleccione **ServiceNow** en la lista de Configuración de adaptador.
7. En la sección Instancias de integración, pulse el icono **Añadir instancia** .

8. Establezca las siguientes opciones.

Opción	Descripción
Nombre	Especifique un nombre para la instancia de ServiceNow.
URL	Especifique el URL para acceder a ServiceNow, por ejemplo, `https://<IP-aplicación servicenow/nombre de host:puerto>`.
Instancia de microservicio	Seleccione la instancia de microservicio necesaria para la integración.
Nombre de usuario	Especifique el nombre de usuario de ServiceNow con el rol de administrador.
Contraseña	Especifique la contraseña para el nombre de usuario.
Habilitar autenticación OAth	Seleccione esta opción para habilitar la autenticación OAth.
Clave secreta de cliente ServiceNow	Especifique la clave secreta.
ID de cliente ServiceNow	Especifique el ID de cliente.

9. Pulse **Guardar** para guardar los detalles de configuración.

Qué hacer a continuación
Para la instancia de adaptador que ha creado, puede probar la conectividad. Seleccione la instancia en la lista de **Instancias de integración** y, a continuación, pulse **Probar conexión** para probar si la comunicación entre la instancia de ServiceNow y el servidor IBM Data Risk Manager es satisfactoria.

Importar CMDB de ServiceNow a IBM Data Risk Manager
Utilice el componente Modelador de contexto empresarial de IBM Data Risk Manager para importar los datos de la base de datos de gestión de configuración (CMDB) de ServiceNow a IBM Data Risk Manager.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con ServiceNow. Para obtener información sobre la integración, consulte "Integración de ServiceNow con IBM Data Risk Manager" en la página 74.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**.
4. Pulse **Cargar desde ServiceNow**.
5. Pulse **Renovar**.
6. Pulse **Sí** para renovar los datos desde ServiceNow.

Integración de IBM InfoSphere Information Governance Catalog con IBM Data Risk Manager

Configure IBM Data Risk Manager ´para que se comunique con IBM InfoSphere Information Governance Catalog (IGC) para recibir los activos definidos en el catálogo IGC. La integración proporciona una representación holística de los activos que controlan la información del catálogo.

IBM Data Risk Manager utiliza el siguiente microservicio para consumir los activos que están definidos en el catálogo IGC.

```
IGC (agente IGC) – se ejecuta en el puerto 8768
```

Requisitos previos

Asegúrese de que tiene la imagen o la compilación del servidor de IBM Data Risk Manager en el formato necesario basándose en el entorno en el que está ejecutando la instalación.

- La versión recomendada de IGC para la integración es 11.7.
- Los activos deben estar asociados solo a los datos estructurados.
- En el catálogo IGC, la relación entre la aplicación y la entidad de activos no es necesaria.
- Los atributos siguientes se deben definir para los activos de tipo `Base de datos` del catálogo IGC admitidos actualmente para la importación en IBM Data Risk Manager.
  - `modified_on`
  - `short_description`
  - `dbms_server_instance`
  - `name`
  - `dbms_version`
  - `dbmsv`
  - `created_by`
  - `dbms_vendor`
  - `created_on`
  - `modified_by`
  - `location`
- Los activos importados del catálogo IGC deben ser mutuamente excluyentes o idénticos a los activos que se cargan a través de otros archivos sin formato como, por ejemplo, los informes de CMDB utilizando el componente de modelado de contexto empresarial de IBM Data Risk Manager.

Flujo de trabajo

- Después de la configuración de integración de IGC en IBM Data Risk Manager, importe los activos definidos en el catálogo IGC.
- Los activos que se importan utilizando el atributo `label` se deben definir para todos los términos planificados para la importación.
- Los términos se deben categorizar en IGC basándose en la taxonomía seleccionada.
  - Todos los términos que están relacionados lógicamente se deben agrupar utilizando categorías IGC.
  - Establezca el campo **Categorías de referencia** con la categoría adecuada para el término respectivo.
- Todos los términos deben tener activos asignados y solo se importan esos activos.
- Flujo de trabajo: **Etiquetas** > **Activos (columnas)** > **Detalles de base de datos**, por ejemplo, **esquemas**.

Integración de IGC con IBM Data Risk Manager

Configure IBM Data Risk Manager para que se comunique con IGC. Para obtener información sobre los pasos de configuración, consulte “Integración de IBM InfoSphere Information Governance Catalog con IBM Data Risk Manager” en la página 77.

Importación de activos definidos en el catálogo IGC

Importe los activos definidos en el catálogo IGC. Para ver los pasos de importación, consulte "Importación de activos definidos en IBM InfoSphere Information Governance Catalog" en la página 79.

Exportación de activos etiquetados a taxonomía

Exporte activos etiquetados para la asignación y publicación de la taxonomía. Para ver los pasos sobre cómo realizar la exportación, consulte "Exportación de activos etiquetados a taxonomía" en la página 79.

Importar datos de contexto

Puede importar los datos de contexto empresarial en IBM Data Risk Manager utilizando uno o varios archivos en formato de valores separados por comas (CSV).

1. Asegúrese de que la base de datos, la aplicación y las hojas de proceso empresarial se editan para los activos definidos en el catálogo IGC.
2. Importe la hoja de datos de contexto.
3. Asegúrese de que los datos de contexto se guardan correctamente y que los atributos se correlacionan con el inventario adecuado para el que las tablas se etiquetan en **Centro de control y mandatos de seguridad** > **Análisis** > **Entorno de trabajo de análisis**.

Para obtener más información sobre la correlación de datos de contexto empresarial, consulte "Correlación de datos de contexto empresarial" en la página 106.

Exportación de activos de datos al panel de control de IBM Data Risk Manager

Para ver los pasos sobre cómo exportar activos al panel de control, consulte "Correlación de taxonomías" en la página 147.

Validación de activos de información en el panel de control de IBM Data Risk Manager

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú  .
3. Pulse **Panel de control**.
4. Seleccione el activo de información adecuado.
5. Valide los detalles de **Infraestructura**, **Partes interesadas**, **Procesos** y **Aplicación**.
6. Pulse el icono **Detalles de activo**  para validar los atributos de IGC correlacionados.

Para obtener más información sobre el panel de control de IBM Data Risk Manager, consulte "Panel de control de IBM Data Risk Manager" en la página 177.

Integración de IBM InfoSphere Information Governance Catalog con IBM Data Risk Manager

Configure IBM Data Risk Manager para que se comunique con IBM InfoSphere Information Governance Catalog para importar los metadatos en IBM Data Risk Manager.

Acerca de esta tarea

El componente Modelador de contexto empresarial (BCM) de IBM Data Risk Manager proporciona el Asistente de integración de empresa para integrar IBM InfoSphere Information Governance Catalog con IBM Data Risk Manager.

Kafka es una cola de mensajes para recibir notificaciones en directo de IBM InfoSphere Information Governance Catalog y IBM Data Risk Manager. En esta cola, IBM InfoSphere Information Governance Catalog es el productor y IBM Data Risk Manager es el consumidor. Puede configurar IBM Data Risk

Manager para suscribirse a los temas de IBM InfoSphere Information Governance Catalog y recibir notificaciones de forma regular para procesar los mensajes.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
4. En la sección Configuración del adaptador, pulse el icono **Añadir adaptador de integración** .
5. Seleccione **IBM Information Governance Catalog** en la lista.
6. Para añadir una instancia de IBM InfoSphere Information Governance Catalog, seleccione **IBM Information Governance Catalog** en la lista de Configuración de adaptador.
7. En la sección Instancias de integración, pulse el icono **Añadir instancia** .
8. Establezca las siguientes opciones.

Opción	Descripción
Nombre	Especifique un nombre para la instancia de IBM InfoSphere Information Governance Catalog.
URL	Especifique el URL para acceder a IBM InfoSphere Information Governance Catalog, por ejemplo, `https://<IP-aplicación information governance catalog/nombre de host:puerto>`.
Instancia de microservicio	Seleccione la instancia de microservicio necesaria para la integración.
Versiones de CIG	Seleccione una versión de IBM InfoSphere Information Governance Catalog para importar metadatos.
Nombre de usuario	Especifique el nombre de usuario de IBM InfoSphere Information Governance Catalog con el rol de administrador.
Contraseña	Especifique la contraseña para el nombre de usuario.

9. Para configurar IBM Data Risk Manager para suscribirse a temas de IBM InfoSphere Information Governance Catalog y recibir notificaciones de forma regular para procesar mensajes, pulse **Configuración de Kafka** y, a continuación, especifique la información de configuración.

Opción	Descripción
Servidor de programa de arranque	Especifique los detalles de host o puerto que se deben utilizar para establecer la conexión inicial al servidor Kafka.
Tema IGC	Especifique el nombre del tema de Kafka en el que se publican los mensajes.
ID de grupo	Especifique el ID de grupo para publicar mensajes cuando se utilizan varios nodos de consumidor Kafka.
Nombre de usuario	Especifique el nombre de usuario que se debe autenticar con el servidor Kafka.
Contraseña	Especifique la contraseña para el nombre de usuario.
Marcar para supresión	Seleccione esta opción para suprimir o eliminar la configuración del servidor Kafka.

10. Pulse **Guardar** para guardar los detalles de configuración.

Qué hacer a continuación
Para la instancia de adaptador que ha creado, puede probar la conectividad. Seleccione la instancia en la lista de **Instancias de integración** y, a continuación, pulse **Probar conexión** para probar si la comunicación entre la instancia de IBM InfoSphere Information Governance Catalog y el servidor IBM Data Risk Manager es satisfactoria.

Importación de activos definidos en IBM InfoSphere Information Governance Catalog
Puede importar los datos de catálogo (activos) que están definidos en el catálogo de IBM InfoSphere Information Governance Catalog (IGC) en el inventario de IBM Data Risk Manager para el análisis de riesgos.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con IGC. Para obtener información sobre la integración, consulte "Integración de IBM InfoSphere Information Governance Catalog con IBM Data Risk Manager" en la página 77.

Procedimiento

1. Identifique los activos de datos confidenciales junto con los términos de IGC (catálogo) y asigne las etiquetas.
2. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
3. Pulse el icono de menú de aplicación .
4. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Exploraciones de datos**.
5. Importar activos.
   a) Pulse el icono **Descargar** .
   b) En la lista **Adaptador**, seleccione **Information Governance Catalog**
   c) En la lista **Instancias**, seleccione una instancia de adaptador.
6. Seleccione el nombre del microservicio IGC, la etiqueta y la categoría en las listas desplegables respectivas para datos estructurados y no estructurados.
7. Pulse **Importar**.

Exportación de activos etiquetados a taxonomía
Exporte los activos etiquetados para la asignación y publicación de la taxonomía.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú .
3. Vaya a **Centro de control y mandatos de seguridad** > **Análisis**.
4. Seleccione la base de datos adecuada que sea relevante para IBM InfoSphere Information Governance Catalog.
5. Valide las tablas etiquetadas.
6. Para exportar el conjunto filtrado de elementos de datos, pulse el icono **Exportar a taxonomía** .
7. Cuando se le solicite, pulse **Sí** para exportar los conjuntos de datos a la taxonomía.
8. Pulse el icono **Exportado** 245 para ver las tablas exportadas.

Qué hacer a continuación
Vaya a **Centro de control y mandatos de seguridad** > **Taxonomía** para validar si la operación de exportación se ha realizado correctamente.

Integración de Imperva SecureSphere con IBM Data Risk Manager

Configure IBM Data Risk Manager para que se conecte e interactúe con Imperva SecureSphere para importar información de vulnerabilidad en IBM Data Risk Manager.

IBM Data Risk Manager utiliza Fullstack para consumir las vulnerabilidades de Imperva SecureSphere.

Asegúrese de que tiene la imagen de IBM Data Risk Manager Server o que el build está disponible en el formato necesario, en función del entorno en el que está ejecutando la instalación.

Para importar datos de vulnerabilidad de Imperva SecureSphere a IBM Data Risk Manager, ejecute las tareas siguientes.

- Importación de la evaluación de vulnerabilidad de Imperva SecureSphere a IBM Data Risk Manager.
  - Evaluación
  - Integración de Imperva SecureSphere con IBM Data Risk Manager.
  - Importación de pruebas de evaluación de vulnerabilidades.
  - Importación de vulnerabilidades en IBM Data Risk Manager.
  - Importar vulnerabilidades como un archivo CSV a IBM Data Risk Manager.
- Importación de resultados de exploración de clasificaciones de Imperva SecureSphere a IBM Data Risk Manager.
  - Descubrimiento y clasificación de Imperva SecureSphere.
  - Importación de resultados del clasificador de Imperva SecureSphere a IBM Data Risk Manager a través del catálogo nativo.

Evaluación

Secure Sphere Assessment Server le permite importar exploraciones de proveedores terceros como, por ejemplo, IBM AppScan, HP Web Inspect, NTObjectives, ImmuniWeb, acunetix y White Hat para listar las vulnerabilidades en el entorno de trabajo de vulnerabilidad de Secure Sphere. Secure Sphere integra Common Vulnerabilities Scoring System (CVSS) que mantiene National Institute of Standards and Technology. El sistema de puntuación puntúa cada vulnerabilidad en una escala de 0 a 10 basándose en el efecto que tiene la vulnerabilidad y el esfuerzo que se precisa utilizarlo.

Integración de Imperva SecureSphere con IBM Data Risk Manager

Para ver los pasos de integración, consulte “Integración de Imperva SecureSphere con IBM Data Risk Manager” en la página 81.

Importar pruebas de evaluación de vulnerabilidades (VA) de Imperva SecureSphere

Para ver los pasos sobre cómo importar pruebas VA, consulte “Importar pruebas de evaluación de vulnerabilidades de Imperva SecureSphere” en la página 81.

Importar vulnerabilidades de Imperva SecureSphere a IBM Data Risk Manager

Para ver los pasos sobre cómo importar vulnerabilidades, consulte Importar exploraciones de vulnerabilidades.

Importación de vulnerabilidades de Imperva SecureSphere como archivo CSV en IBM Data Risk Manager

Puede importar vulnerabilidades como un archivo CSV a IBM Data Risk Manager. Para ver los pasos sobre cómo importar el archivo CSV, consulte Importar exploraciones de vulnerabilidades.

Descubrimiento y clasificación de Secure Sphere

El descubrimiento y la clasificación de Secure Sphere proporciona un conjunto de herramientas que le ayuda a descubrir servicios web. A continuación, utilice esta información de clasificación para crear políticas de seguridad para supervisarlas y alertarle sobre actividades sospechosas.

La ventana Descubrimiento y clasificación proporciona una amplia selección de opciones que le permiten navegar entre las características disponibles para configurar exploraciones y visualizar el servidor descubierto.

Puede desencadenar la exploración de clasificación en Imperva SecureSphere y los resultados pueden exportarse a un archivo CSV. Estos contenidos se pueden personalizar utilizando la plantilla de clasificador de catálogo nativo de IBM Data Risk Manager y se pueden importar a IBM Data Risk Manager.

Importación de los resultados de clasificador de Imperva SecureSphere a IBM Data Risk Manager

Para ver los pasos sobre cómo importar el archivo CSV de resultados del clasificador (datos de catálogo) a IBM Data Risk Manager, consulte "Importar el archivo CSV de resultados del clasificador (datos de catálogo) a IBM Data Risk Manager" en la página 43.

Integración de Imperva SecureSphere con IBM Data Risk Manager

Debe configurar IBM Data Risk Manager para que se conecte e interactúe con Imperva SecureSphere para importar información de vulnerabilidad en IBM Data Risk Manager.

Acerca de esta tarea

El componente Modelador de contexto empresarial (BCM) de IBM Data Risk Manager proporciona el Asistente de integración de empresa para integrar Imperva SecureSphere con IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
4. En la sección Configuración del adaptador, pulse el icono **Añadir adaptador de integración** .
5. Seleccione **Imperva** en la lista.
6. Para añadir una instancia de Imperva SecureSphere, seleccione **Imperva** en la lista de Configuración de adaptador.
7. En la sección Instancias de integración, pulse el icono **Añadir instancia** .
8. Establezca las siguientes opciones.

Opción	Descripción
Nombre	Especifique un nombre para la instancia de Imperva SecureSphere.
URL	Especifique el URL para acceder a Imperva SecureSphere, por ejemplo, `https://<IP-aplicación imperva/nombre de host:puerto>`.
Nombre de usuario	Especifique el nombre de usuario de Imperva SecureSphere con el rol de administrador.
Contraseña	Especifique la contraseña para el nombre de usuario.

9. Pulse **Guardar** para guardar los detalles de configuración.

Importar pruebas de evaluación de vulnerabilidades de Imperva SecureSphere

Importe pruebas de evaluación de vulnerabilidades (VA) de Imperva SecureSphere en IBM Data Risk Manager para su análisis.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de navegación de la aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Pruebas VA**.
4. Para descargar las plantillas de exploración, pulse el icono de descarga .
5. En la ventana **Importar**, seleccione la instancia de adaptador para Imperva SecureSphere.
6. Pulse **Importar**. Cuando la operación de importación se haya completado, las pruebas VA se añaden al inventario.
7. Para renovar la lista de inventario de pruebas VA, pulse el icono **Renovar** .

Importar vulnerabilidades de Imperva SecureSphere a IBM Data Risk Manager

Puede importar exploraciones de vulnerabilidad desde dispositivos Imperva SecureSphere en el inventario de IBM Data Risk Manager para el análisis de riesgos.

Antes de empezar

Cuando se importan las exploraciones, también se importan los resultados de la exploración. Asegúrese de importar los sitios desde Imperva SecureSphere primero.

Acerca de esta tarea

El icono de transacción indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Exploraciones de datos**.
4. Importe las exploraciones de datos.
   a) Pulse el icono **Descargar** .
   b) En la ventana **Importar**, seleccione **Evaluación de vulnerabilidad**.
   c) En la lista **Adaptador**, seleccione **Imperva**.
   d) En la lista **Adaptadores**, seleccione una instancia de adaptador. Puede seleccionar hasta tres instancias.
   e) Seleccione la fecha a partir de la cual desea extraer las exploraciones de vulnerabilidades desde Imperva SecureSphere.
   f) Pulse **Importar**. Cuando la operación de importación se haya completado, las exploraciones de vulnerabilidades de Imperva SecureSphere se añaden al inventario.
   g) Para renovar la lista de inventario de exploraciones de datos, pulse el icono **Renovar** .
5. Para ver los resultados de la exploración después de la operación de importación, vaya a **Centro de control y mandatos de seguridad** > **Inicio**.

Importar vulnerabilidades como un archivo CSV a IBM Data Risk Manager
Utilice el componente Modelador de contexto empresarial de IBM Data Risk Manager para importar las vulnerabilidades como un archivo CSV a IBM Data Risk Manager.

Antes de empezar

Asegúrese de que los datos de contexto empresarial estén disponibles para importarlos.

Puede descargar las plantillas de ejemplo en: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**.
4. Habilite el botón de conmutación **Datos de catálogo**.
5. Seleccione **Vulnerabilidad**.
6. Pulse **Elegir archivo** para localizar y seleccionar el archivo.
7. Pulse **Cargar**.
   Los datos se visualizan para su verificación.
8. Pulse **Importar**.

Importar el archivo CSV de resultados del clasificador (datos de catálogo) a IBM Data Risk Manager
Utilice el componente Modelador de contexto empresarial de IBM Data Risk Manager para importar los resultados del clasificador como un archivo CSV a IBM Data Risk Manager.

Antes de empezar

Asegúrese de que los datos de contexto empresarial estén disponibles para importarlos.

Puede descargar las plantillas de ejemplo en: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**.
4. Habilite el botón de conmutación **Datos de catálogo**.
5. Seleccione **Clasificación**.
6. Pulse **Elegir archivo** para localizar y seleccionar el archivo.
7. Pulse **Cargar**.
   Los datos se visualizan para su verificación.
8. Pulse **Importar**.

Integración de IBM Multi-Cloud Data Encryption con IBM Data Risk Manager

Configure IBM Data Risk Manager para conectarse e interactuar con IBM Multi-Cloud Data Encryption para captar detalles de cifrado de orígenes de datos añadidos al inventario de distintos orígenes donde está desplegado el agente de IBM Multi-Cloud Data Encryption para el cifrado de datos.

Asegúrese de que tiene la imagen de IBM Data Risk Manager Server o que el build está disponible en el formato necesario, en función del entorno en el que está ejecutando la instalación.

Para captar y visualizar el estado de cifrado de los orígenes de datos en IBM Data Risk Manager, ejecute las tareas siguientes.

Integración de IBM Multi-Cloud Data Encryption con IBM Data Risk Manager

Para ver los pasos de integración, consulte "Integración de IBM Multi-Cloud Data Encryption con IBM Data Risk Manager" en la página 84.

Captar el estado de IBM Multi-Cloud Data Encryption

Para ver los pasos sobre cómo añadir detalles de cifrado de los orígenes de datos, consulte "Captar el estado de IBM Multi-Cloud Data Encryption de orígenes de datos" en la página 85.

Visualización del estado de cifrado de IBM Multi-Cloud Data Encryption en el panel de control

Puede ver el estado de cifrado de los orígenes de datos que ha captado de IBM Multi-Cloud Data Encryption en el widget **Infraestructura** del panel de control de IBM Data Risk Manager. Para ver los pasos sobre cómo ver el estado en el panel de control, consulte "Visualización del estado de cifrado de IBM Multi-Cloud Data Encryption en el panel de control" en la página 85.

Integración de IBM Multi-Cloud Data Encryption con IBM Data Risk Manager

Debe configurar IBM Data Risk Manager para conectarse e interactuar con IBM Multi-Cloud Data Encryption para captar detalles de cifrado de orígenes de datos añadidos al inventario de distintos orígenes donde está desplegado el agente de IBM Multi-Cloud Data Encryption para el cifrado de datos.

Acerca de esta tarea

El componente Modelador de contexto empresarial (BCM) de IBM Data Risk Manager proporciona el Asistente de integración de empresa para integrar IBM Multi-Cloud Data Encryption con IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
4. En la sección Plataformas de integración, pulse el icono **Añadir adaptador de integración** .
5. Seleccione **IBM MDE** en la lista.
6. Para añadir una instancia de IBM Multi-Cloud Data Encryption, seleccione **IBM MDE** en la lista de Plataformas de integración.
7. En la sección Instancias de integración, pulse el icono **Añadir instancia** .
8. Establezca las siguientes opciones.

Opción	Descripción
Nombre	Especifique el nombre de instancia de IBM Multi-Cloud Data Encryption.
URL	Especifique el URL para acceder a IBM Multi-Cloud Data Encryption, por ejemplo `https://<IP-servidor MDE/nombre de host:puerto>`.
Instancia de microservicio	Seleccione la instancia de microservicio necesaria para la integración.
Nombre de usuario	Especifique el nombre de usuario de IBM Multi-Cloud Data Encryption con el rol de administrador.
Contraseña	Especifique la contraseña para el nombre de usuario.

Opción	Descripción
Clasificador y evaluación de vulnerabilidades	Especifique el archivo de configuración para importar datos del servidor de integración a IBM Data Risk Manager para las evaluaciones de vulnerabilidad y clasificación de datos.

9. Pulse **Guardar** para guardar los detalles de configuración.

Qué hacer a continuación
Para la instancia de adaptador que ha creado, puede probar la conectividad. Seleccione la instancia en la lista de **Instancias de integración** y, a continuación, pulse **Probar conexión** para probar si la comunicación entre la instancia de IBM Multi-Cloud Data Encryption y el servidor IBM Data Risk Manager es satisfactoria.

Captar el estado de IBM Multi-Cloud Data Encryption de orígenes de datos
Capte el estado de IBM Multi-Cloud Data Encryption de orígenes de datos para visualizarlos en el inventario de orígenes de datos de IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de navegación de la aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario**.
4. Pulse **Sincronizar estado de supervisión**.
5. Seleccione el adaptador de IBM Multi-Cloud Data Encryption en la lista **Adaptadores**.
6. Pulse **Renovar**.

   En la ventana Gestionar inventario, si el cifrado está activo para los orígenes de datos del adaptador que ha especificado, se muestra el icono **Cifrado activo** .

Visualización del estado de cifrado de IBM Multi-Cloud Data Encryption en el panel de control
Puede ver el estado de cifrado de los orígenes de datos que ha captado de IBM Multi-Cloud Data Encryption en el widget **Infraestructura** del panel de control de IBM Data Risk Manager.

Antes de empezar
Asegúrese de que IBM Multi-Cloud Data Encryption está integrado con IBM Data Risk Manager para obtener el estado de cifrado. Para ver los pasos de integración, consulte "Integración de IBM Multi-Cloud Data Encryption con IBM Data Risk Manager" en la página 84.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager utilizando sus credenciales.
2. Pulse el icono de menú .
3. Pulse **Panel de control**. Se mostrará la página **Conjunto de activos de información**.
4. Pulse un activo de información para visualizar los widgets del panel de control.
5. En el widget **Infraestructura**, se puede ver el icono , que indica si el estado de cifrado está activo.

Integración de OneTrust con IBM Data Risk Manager

Configure IBM Data Risk Manager para conectarse e interactuar con OneTrust para importar inventarios y su información de riesgo correspondiente en IBM Data Risk Manager. Estos riesgos se correlacionan con los activos de información y la infraestructura correspondientes en IBM Data Risk Manager para visualizarlos en el panel de control para el análisis de riesgo y las acciones.

Asegúrese de que tiene la imagen de IBM Data Risk Manager Server o que el build está disponible en el formato necesario, en función del entorno en el que está ejecutando la instalación.

Puede importar los siguientes tipos de inventario de OneTrust.

- Activos
  - Aplicación
  - Base de datos
  - Almacenamiento físico
  - Sitio web
  - Proveedor
- Actividades de proceso
- Proveedores

Para importar detalles de riesgos y la lista de inventarios de OneTrust a IBM Data Risk Manager, ejecute las tareas siguientes.

Integración de OneTrust con IBM Data Risk Manager

Para ver los pasos de integración, consulte "Integración de OneTrust con IBM Data Risk Manager" en la página 86.

Importación de inventarios e información de riesgos de OneTrust

Para obtener más información sobre cómo importar los inventarios, consulte "Importación de inventarios e información de riesgos de OneTrust" en la página 87.

Visualización de inventarios e información de riesgos de OneTrust en un widget de bienvenida

Para obtener más información sobre cómo ver la información de riesgos, consulte "Visualización de inventarios e información de riesgos de OneTrust en un widget de bienvenida" en la página 87.

Integración de OneTrust con IBM Data Risk Manager

Configure IBM Data Risk Manager para conectarse e interactuar con OneTrust para importar inventarios y su información de riesgo correspondiente en IBM Data Risk Manager.

Acerca de esta tarea

El componente Modelador de contexto empresarial (BCM) de IBM Data Risk Manager proporciona el Asistente de integración de empresa para integrar OneTrust con IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager utilizando sus credenciales de usuario.
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
4. En la sección Plataformas de integración, pulse el icono **Añadir adaptador de integración** .
5. Seleccione **OneTrust** en la lista.
6. Para añadir una instancia de OneTrust, seleccione **OneTrust** en la lista Plataformas de integración.
7. En la sección Instancias de integración, pulse el icono **Añadir instancia** .
8. Establezca las siguientes opciones.

Opción	Descripción
Nombre	Especifique el nombre de instancia de OneTrust.
URL	Especifique el URL de acceso a OneTrust, por ejemplo, `https://ejemplo.com/`.
Instancia de microservicio	Seleccione el agente de integración de la lista.
Clave de API	Especifique la clave de API para importar datos utilizando la API HTTP de OneTrust. Las claves de API se utilizan para autenticar sus solicitudes de la API HTTP.
Clasificador y evaluación de vulnerabilidades	Especifique el archivo de configuración para importar datos del servidor de integración a IBM Data Risk Manager para las evaluaciones de vulnerabilidad y clasificación de datos.

9. Pulse **Guardar** para guardar los detalles de configuración.

Qué hacer a continuación

Para la instancia de adaptador que ha creado, puede probar la conectividad. Seleccione la instancia en la lista de **Instancias de integración** y, a continuación, pulse **Probar conexión** para probar si la comunicación entre la instancia de OneTrust y el servidor IBM Data Risk Manager es satisfactoria.

Importación de inventarios e información de riesgos de OneTrust

Importe inventarios e importación de riesgos de OneTrust en IBM Data Risk Manager para el análisis de riesgos y las acciones.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager utilizando sus credenciales.
2. Pulse el icono de navegación de la aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Riesgo**.
4. Pulse el icono Importar .
5. En la ventana **Importar**, seleccione una instancia de adaptador OneTrust apropiada.
6. Pulse **Importar**.

   La lista de inventarios y la información de riesgos correspondiente de OneTrust se muestran en la página **Evaluación de riesgos**.

Visualización de inventarios e información de riesgos de OneTrust en un widget de bienvenida

Puede ver los datos que ha importado de OneTrust en el widget Distribución de activos de información de la página Imagen de pantalla de bienvenida de privacidad de IBM Data Risk Manager para visualizar y analizar rápidamente la información de riesgos.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager utilizando sus credenciales.
2. Pulse el icono de menú .
3. Pulse **Imagen de pantalla de privacidad**.
4. En el widget **Distribución de activos de información** > **Riesgo de privacidad**, puede ver la información de riesgos en detalle.

Integración de IBM Security Guardium Analyzer con IBM Data Risk Manager

Configure IBM Data Risk Manager para que se conecte e interactúe con IBM Security Guardium Analyzer para importar exploraciones de clasificador e información de vulnerabilidad en IBM Data Risk Manager.

Asegúrese de que tiene la imagen de IBM Data Risk Manager Server o que el build está disponible en el formato necesario, en función del entorno en el que está ejecutando la instalación.

Para importar datos de IBM Security Guardium Analyzer en IBM Data Risk Manager en un análisis de riesgos, ejecute las tareas siguientes.

Importación de orígenes de datos de IBM Security Guardium Analyzer

Para obtener más información sobre cómo importar orígenes de datos, consulte "Importación de orígenes de datos de IBM Security Guardium Analyzer" en la página 89.

Integración de IBM Security Guardium Analyzer con IBM Data Risk Manager

Para ver los pasos de integración, consulte "Integración de IBM Security Guardium Analyzer con IBM Data Risk Manager" en la página 88.

Importación de exploraciones de clasificador desde IBM Security Guardium Analyzer

Para obtener más información sobre cómo importar exploraciones de clasificador, consulte "Importación de exploraciones de clasificador desde IBM Security Guardium Analyzer" en la página 90.

Importación de exploración de vulnerabilidades desde IBM Security Guardium Analyzer

Para obtener más información sobre cómo importar exploraciones de vulnerabilidad, consulte "Importación de exploraciones de vulnerabilidad de IBM Security Guardium Analyzer en IBM Data Risk Manager" en la página 91.

Visualización de los resultados de una exploración de evaluación de vulnerabilidades

Para obtener más información sobre cómo ver los resultados de una exploración de evaluación de vulnerabilidades, consulte "Ver los resultados de la exploración de evaluación de vulnerabilidades de IBM Security Guardium Analyzer" en la página 91.

Correlación de vulnerabilidades de IBM Security Guardium Analyzer en el panel de control de IBM Data Risk Manager

Pulse en la página secundaria de Conjunto de activos de información del panel de control para ver las vulnerabilidades de IBM Security Guardium Analyzer en la pestaña **Vulnerabilidades**. Para obtener más información sobre el panel de control, consulte "Panel de control de IBM Data Risk Manager" en la página 177.

Integración de IBM Security Guardium Analyzer con IBM Data Risk Manager

Configure IBM Data Risk Manager para que se conecte e interactúe con IBM Security Guardium Analyzer a fin de importar exploraciones de clasificador y de evaluación de vulnerabilidades en IBM Data Risk Manager.

Acerca de esta tarea

El componente Modelador de contexto empresarial (BCM) de IBM Data Risk Manager proporciona el Asistente de integración de empresa para integrar IBM Security Guardium Analyzer con IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager utilizando sus credenciales de usuario.

2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
4. En la sección Configuración del adaptador, pulse el icono **Añadir adaptador de integración** .
5. Seleccione **IBM Guardium Analyzer** en la lista.
6. Para añadir una instancia de IBM Security Guardium Analyzer, seleccione **IBM Guardium Analyzer** en la lista de Configuración de adaptador.
7. En la sección Instancias de integración, pulse el icono **Añadir instancia** .
8. Establezca las siguientes opciones.

Opción	Descripción
Nombre	Especifique el nombre de instancia de IBM Security Guardium Analyzer.
URL	Especifique el URL de acceso a IBM Security Guardium Analyzer. Por ejemplo, `https://www.ejemplo.com/`.
Instancia de microservicio	Seleccione el agente de integración de la lista.
Nombre de usuario	Especifique el nombre de usuario de IBM Security Guardium Analyzer.
Contraseña	Especifique la contraseña para el nombre de usuario.
Clasificador y evaluación de vulnerabilidades	Especifique el archivo de configuración para importar datos del servidor de integración a IBM Data Risk Manager para las evaluaciones de vulnerabilidad y clasificación de datos.

9. Pulse **Guardar** para guardar los detalles de configuración.

Qué hacer a continuación
Para la instancia de adaptador que ha creado, puede probar la conectividad. Seleccione la instancia en la lista de **Instancias de integración** y, a continuación, pulse **Probar conexión** para probar si la comunicación entre la instancia de IBM Security Guardium Analyzer y el servidor IBM Data Risk Manager es satisfactoria.

Importación de orígenes de datos de IBM Security Guardium Analyzer
Puede importar orígenes de datos de IBM Security Guardium Analyzer al inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con IBM Security Guardium Analyzer. Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium Analyzer con IBM Data Risk Manager" en la página 88.

Acerca de esta tarea

El icono de transacción indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://`*`<dirección-IP-servidor-IDRM>`*`:8443/albatross/a3suite`).

2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Origen de datos**.
4. Importe orígenes de datos.
   a) Pulse el icono **Descargar** .
   b) En la ventana **Importar**, seleccione una instancia de IBM Security Guardium Analyzer.
   c) Pulse **Importar**.
      Cuando se haya completado la operación de importación, se añadirán los orígenes de datos de IBM Security Guardium Analyzer al inventario.
   d) Para renovar la lista de inventario de orígenes de datos, pulse el icono **Renovar** .

   El origen de datos que ha añadido aparece listado en la página **Origen de datos**. De forma alternativa, también puede ver los orígenes de datos que ha importado en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración de empresarial** > **Gestionar inventario** > **Origen de datos** > **Base de datos**.

Importación de exploraciones de clasificador desde IBM Security Guardium Analyzer
Puede importar exploraciones de clasificador desde IBM Security Guardium Analyzer al inventario de IBM Data Risk Manager para el análisis de riesgos.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con IBM Security Guardium Analyzer. Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium Analyzer con IBM Data Risk Manager" en la página 88.

Acerca de esta tarea

El icono de transacción indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Exploraciones de datos**.
4. Importe las exploraciones de datos.
   a) Pulse el icono **Descargar** .
   b) En la ventana **Importar**, seleccione **Clasificador**.
   c) Desde la lista **Adaptador**, seleccione **IBM Guardium Analyzer**.
   d) En la lista **Instancias**, seleccione una instancia de adaptador. Puede seleccionar hasta tres instancias.
   e) Pulse **Importar**. Cuando la operación de importación se haya completado, las exploraciones de clasificador de IBM Security Guardium Analyzer se añaden al inventario.

f) Para renovar la lista de inventario de exploraciones de datos, pulse el icono **Renovar**  .

5. De forma alternativa, para ver los resultados de exploración después de la operación de importación, vaya a **Centro de control y mandatos de seguridad** > **Inicio**.

Importación de exploraciones de vulnerabilidad de IBM Security Guardium Analyzer en IBM Data Risk Manager

Puede importar exploraciones de vulnerabilidades desde IBM Security Guardium Analyzer al inventario de IBM Data Risk Manager para el análisis de riesgos.

Acerca de esta tarea

El icono de transacción  indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción  indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Exploraciones de datos**.
4. Importe las exploraciones de datos.
   a) Pulse el icono **Descargar**  .
   b) En la ventana **Importar**, seleccione **Evaluación de vulnerabilidad**.
   c) Desde la lista **Adaptador**, seleccione **IBM Guardium Analyzer**.
   d) En la lista **Instancias**, seleccione una instancia de adaptador. Puede seleccionar hasta tres instancias.
   e) Pulse **Importar**. Cuando se haya completado la operación de importación, las exploraciones de evaluación de vulnerabilidades de IBM Security Guardium Analyzer se añaden al inventario.
   f) Para renovar la lista de inventario de exploraciones de datos, pulse el icono **Renovar**  .
5. De forma alternativa, para ver los resultados de exploración después de la operación de importación, vaya a **Centro de control y mandatos de seguridad** > **Inicio**.

Ver los resultados de la exploración de evaluación de vulnerabilidades de IBM Security Guardium Analyzer

Utilice el componente Evaluación de vulnerabilidades de IBM Data Risk Manager para ver los resultados de la exploración de evaluación de vulnerabilidades para un análisis y acciones adicionales.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Pulse **Gestión de vulnerabilidades**.
4. Pulse **Ver resultados**.
5. Pulse en el icono de filtro  en **Orígenes de datos VA** y seleccione el tipo de adaptador como, por ejemplo, `IBM Guardium Analyzer`.

6. En la evaluación seleccionada, pulse en el número de **Pasado**, **Fallo** u **Otros** para visualizar los resultados en la página **Resultados de prueba de vulnerabilidades**.
7. Para ver los resultados por plataforma de base de datos, pulse **Plataformas VA**.

Integración de IBM StoredIQ con IBM Data Risk Manager

Configure IBM Data Risk Manager para conectarse con e interactuar con IBM StoredIQ para utilizar sus resultados de datos de clasificación para el análisis de riesgos y acciones. IBM StoredIQ proporciona un análisis escalable y el control de datos no estructurados en su sitio entre sitios distintos y distribuidos de correo electrónico, comparticiones de archivos, escritorios y de colaboración.

Un volumen representa un origen de datos o un destino que está disponible en la red para IBM StoredIQ. Un conjunto de datos puede contener varios volúmenes. El conjunto de datos es el concepto principal en el uso de las aplicaciones IBM StoredIQ. Se crea y utiliza para recopilar datos específicos para gestionar el sistema empresarial. La función de creación de informes proporciona vistas externas del conjunto de datos y valida procesos de IBM StoredIQ. Puede compartir la información que está incluida dentro del conjunto de datos con el componente de creación de informes, lo que permite que el conjunto de datos se transfiera a otros tipos de soporte para la revisión y el análisis. Actualmente, puede importar solo el informe **Exportación de detalles de acierto de término CSV** en IBM Data Risk Manager para el análisis de datos.

Para obtener más información sobre IBM StoredIQ, consulte la documentación del producto en: https://www.ibm.com/support/knowledgecenter/SSSHEC_7.6.0/welcome/storediq.html

Para importar datos desde IBM StoredIQ a IBM Data Risk Manager, ejecute las tareas siguientes.

Integración de IBM StoredIQ con IBM Data Risk Manager

Para ver los pasos de integración, consulte “Integración de IBM StoredIQ con IBM Data Risk Manager” en la página 92.

Importación de orígenes de datos de IBM StoredIQ

Para obtener más información sobre cómo importar orígenes de datos, consulte “Importación de orígenes de datos de IBM StoredIQ” en la página 93.

Importación de exploraciones de clasificador desde IBM StoredIQ

Para obtener más información sobre cómo importar exploraciones de clasificador, consulte “Importación de exploraciones de clasificador desde IBM StoredIQ” en la página 94.

Correlación de los datos de resultados de clasificación con la infraestructura en el panel de control de IBM Data Risk Manager

1. Cuando las exploraciones de IBM StoredIQ se importan correctamente, los activos que están asociados al origen de datos están disponibles en **Centro de control y mandatos de seguridad** > **Taxonomía** > **Sin estructura** > **Activos recién descubiertos**. Seleccione los activos.
2. Aplique los atributos primario y secundario apropiados.
3. Exporte los activos de información no estructurada al panel de control de IBM Data Risk Manager.
4. Los resultados del clasificador correspondiente se correlacionan con la infraestructura apropiada en el panel de control de IBM Data Risk Manager.

Integración de IBM StoredIQ con IBM Data Risk Manager

Configure IBM Data Risk Manager para conectarse con e interactuar con IBM StoredIQ para utilizar sus resultados de datos de clasificación para el análisis de riesgos y acciones.

Acerca de esta tarea

El componente Modelador de contexto empresarial (BCM) de IBM Data Risk Manager proporciona el Asistente de integración de empresa para integrar IBM StoredIQ con IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager utilizando sus credenciales de usuario.
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
4. En la sección Configuración del adaptador, pulse el icono **Añadir adaptador de integración** .
5. Seleccione **Stored IQ** en la lista.
6. Para añadir una instancia de IBM StoredIQ, seleccione **Stored IQ** en la lista de Configuración de adaptador.
7. En la sección Instancias de integración, pulse el icono **Añadir instancia** .
8. Establezca las siguientes opciones.

Opción	Descripción
Nombre	Especifique el nombre de instancia de IBM StoredIQ.
URL	Especifique el URL de acceso a IBM StoredIQ. Por ejemplo, `https://www.example.com/login`.
Instancia de microservicio	Seleccione el agente de integración de la lista.
Nombre de usuario	Especifique el nombre de usuario de IBM StoredIQ.
Contraseña	Especifique la contraseña para el nombre de usuario.
Clasificador y evaluación de vulnerabilidades	Especifique el archivo de configuración para importar datos desde el servidor de integración a IBM Data Risk Manager para el análisis de riesgos y acciones.

9. Pulse **Guardar** para guardar los detalles de configuración.

Qué hacer a continuación

Para la instancia de adaptador que ha creado, puede probar la conectividad. Seleccione la instancia en la lista de **Instancias de integración** y, a continuación, pulse **Probar conexión** para probar si la comunicación entre la instancia de IBM StoredIQ y el servidor IBM Data Risk Manager es satisfactoria.

Importación de orígenes de datos de IBM StoredIQ

Puede importar orígenes de datos no estructurados desde IBM StoredIQ al inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM StoredIQ. Para obtener más información sobre la integración, consulte “Integración de IBM StoredIQ con IBM Data Risk Manager” en la página 92.

Acerca de esta tarea

El icono de transacción indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Origen de datos**.
4. Importe orígenes de datos.
   a) Pulse el icono **Descargar**  .
   b) En la ventana **Importar**, seleccione una instancia de IBM StoredIQ.
   c) Pulse **Importar**.
      Cuando se haya completado la operación de importación, se añadirán los orígenes de datos de IBM StoredIQ al inventario.
   d) Para renovar la lista de inventario de orígenes de datos, pulse el icono **Renovar**  .

   El origen de datos que ha añadido aparece listado en la página **Origen de datos**. De forma alternativa, también puede ver los orígenes de datos que ha importado en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Almacenamiento de archivos**.

Importación de exploraciones de clasificador desde IBM StoredIQ
Puede importar exploraciones de clasificador desde IBM StoredIQ a IBM Data Risk Manager para el análisis de riesgos.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con IBM StoredIQ. Para obtener más información sobre la integración, consulte "Integración de IBM StoredIQ con IBM Data Risk Manager" en la página 92.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Exploraciones de datos**.
4. Importe las exploraciones de datos.
   a) Pulse el icono **Descargar**  .
   b) En la ventana **Importar exploraciones de datos**, desde la lista **Adaptador**, seleccione **StoredIQ**.
   c) En la lista **Instancias**, seleccione una instancia de adaptador. Puede seleccionar hasta tres instancias.
   d) Seleccione **Clasificador**.
   e) Para importar todos los procesos que están asociados a las instancias seleccionadas, pulse **Importar**.
   f) Para importar solo los procesos de IBM StoredIQ que necesita de las instancias seleccionadas, ejecute los pasos siguientes.
      1) Pulse **Importar con selección de procesos**.
      2) Seleccione los procesos que necesaria importar de cada instancia de adaptador.

3) Pulse **Importar**.

5. En la página **Exploraciones de datos**, puede ver las exploraciones que ha importado ahora.
6. Para renovar la lista de inventario de exploraciones de datos, pulse el icono **Renovar**  .
7. De forma alternativa, para ver los resultados de exploración después de la operación de importación, vaya a **Centro de control y mandatos de seguridad** > **Inicio**.

Administración de usuarios

La administración de usuarios cubre las tareas de añadir y mantener usuarios y grupos de IBM Data Risk Manager y asociar usuarios a roles para realizar tareas específicas dentro de las aplicaciones.

Roles de usuario predefinidos de IBM Data Risk Manager

Un rol es un objeto que define los niveles de autorización necesarios para realizar las funciones de producto. Para permitir que los usuarios accedan a las funciones de producto, se deben correlacionar con los roles de usuario. Esta correlación permite a los usuarios acceder a los componentes de IBM Data Risk Manager definidos por el rol.

Los siguientes roles de usuario se definen en IBM Data Risk Manager:

- Roles de administrador
- Roles generales

Roles de administrador

El rol de administrador proporciona control sobre todas las funciones de Suite de aplicaciones de IBM Data Risk Manager. Los distintos roles de administrador se describen en las secciones siguientes.

Superadministrador
El rol de superadministrador proporciona control sobre todas las funciones y subfunciones de Suite de aplicaciones de IBM Data Risk Manager. Además, el superadministrador es responsable de las funciones de administración de servidor siguientes:

- Gestión de licencias
- Configuración del adaptador de integración
- Configuración del servidor

Administrador de BCM
El rol de administrador de BCM proporciona control sobre todas las funciones del componente Modelador de contexto empresarial (BCM) de Suite de aplicaciones de IBM Data Risk Manager. El administrador de BCM actúa como administrador de seguridad de IBM Data Risk Manager y es responsable de las actividades de registro de usuarios, gestión de usuarios y asignación de roles. Además, el administrador de BCM es responsable de las tareas siguientes.

- Integración empresarial
- Gestión de programas
- Gestión de políticas
- Exploraciones de evaluación de vulnerabilidades

Administrador de C3
El rol de administrador de C3 proporciona control sobre todas las funciones del componente Centro de control y mandatos de seguridad de Suite de aplicaciones de IBM Data Risk Manager. El administrador de C3 es responsable de las actividades siguientes.

- Planificación y desencadenado de exploraciones de descubrimiento
- Visualización, exportación y gestión de la reparación de evaluaciones de vulnerabilidades

Administrador de IDRM
El rol de administrador de IDRM proporciona control sobre todas las funciones del componente Centro de control y mandatos de seguridad de Suite de aplicaciones de IBM Data Risk Manager. Además de las funciones de panel de control generales, el administrador de IDRM es responsable de enviar notificaciones por correo electrónico sobre las alertas de supervisión de actividad de base de datos (DAM).

Roles generales

Los roles generales proporcionan acceso a las funciones básicas de usuario de los componentes de Suite de aplicaciones de IBM Data Risk Manager.

General de BCM
El rol general de BCM proporciona acceso a las funciones de uso general siguientes del componente BCM.

- Descubrimiento de orígenes de datos nativos
- Modelado de flujo de datos o modelado de contexto empresarial
- Gestión de reparaciones

General de C3
El rol general de C3 proporciona acceso a las siguientes funciones de uso general del componente Centro de control y mandatos de seguridad.

- Gestión de inventario
- Limpieza y análisis iterativos
- Definición de taxonomía
- Centro de acción

General de IDRM
El rol general de IDRM proporciona acceso a las funciones de uso general del panel de control de IBM Data Risk Manager.

Gestión de usuarios

Con la función de gestión de usuarios de IBM Data Risk Manager, los administradores pueden crear usuarios, asignar roles de usuario, actualizar la información de usuario y cambiar una contraseña de usuario.

El servidor de IBM Data Risk Manager almacena información acerca de los usuarios que pueden acceder a varios componentes de IBM Data Risk Manager. Tanto la autenticación como los procesos de autorización utilizan la información de usuario. El componente Modelador de contexto empresarial (BCM) proporciona el Asistente de integración empresarial (EIW) para crear y gestionar usuarios.

El rol de administrador de BCM es necesario para realizar las funciones de gestión de usuarios.

Crear una cuenta de usuario

Puede crear usuarios y proporcionarles acceso a IBM Data Risk Manager. Utilice el Asistente de integración empresarial del Modelador de contexto empresarial para crear usuarios y gestionar sus permisos.

Antes de empezar

Debe tener el rol de administrador de BCM para llevar a cabo las funciones de gestión de usuarios.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de navegación de la aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Usuario**.

4. Para crear un usuario, pulse el icono **Añadir usuario**  .
5. Establezca las opciones siguientes y pulse **Guardar**.

Opción	Descripción
Tipo de usuario	Puede especificar cualquiera de los siguientes tipos para iniciar sesión en IBM Data Risk Manager. • **Usuario de IDRM** • **Inicio de sesión único** • **LDAP**
Nombre de usuario	Especifique el nombre del usuario.
Contraseña	Especifique la contraseña para el nombre de usuario.
Volver a escribir contraseña	Confirme la contraseña.
Nombre de recurso	Especifique el nombre del recurso para el usuario que va a crear. Para obtener información sobre cómo crear el nombre de recurso, consulte "Creación de un recurso para asociarlo al usuario" en la página 97.
Correo electrónico	Especifique la dirección de correo electrónico del recurso. Para obtener información sobre cómo especificar el nombre de recurso, consulte "Creación de un recurso para asociarlo al usuario" en la página 97.
Roles	Asigne un rol al usuario que va a crear.
Asignar programa(s)	Asigne programas al usuario. Ejecute los pasos siguientes para asignar programas. Para obtener más información sobre los programas, consulte "Gestión de programas" en la página 133. a. Pulse **Asignar programa(s)**. b. Seleccione los programas que desea asignar. **Nota:** No puede asignar un programa para el usuario con **Superadministrador**.

Creación de un recurso para asociarlo al usuario

Debe añadir un recurso y asociarlo a la credencial de usuario de IBM Data Risk Manager que está creando. Para añadir un recurso, debe especificar el nombre de recurso y el ID de correo electrónico para el nombre de recurso.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de navegación de la aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **EIW** > **Usuario**.
4. Para crear un usuario, pulse el icono **Añadir usuario**  .
5. Especifique el nombre del usuario.
6. Especifique los detalles de contraseña.
7. Para crear un nombre de recurso y el correo electrónico para el usuario que está creando, pulse el icono **Nombre de recurso**  .
   a) En la página Recursos, pulse el icono Añadir recurso  .
   b) Especifique el nombre del recurso que desea asociar al usuario que está creando.

c) Especifique el ID de correo electrónico del nombre de recurso.

d) Pulse **Enviar**.

Se mostrarán el nombre del recurso y el ID de correo electrónico en los campos **Nombre de recurso** y **Correo electrónico**.

También puede asociar un nombre de recurso existente al usuario. Además, puede modificar los detalles de nombre del recurso.

8. Pulse **Guardar**.

Modificación de la información del usuario

Puede modificar los usuarios existentes, incluidos sus estados según sea necesario. También puede activar los usuarios inhabilitados en IBM Data Risk Manager.

Antes de empezar

Debe tener el rol de administrador de BCM para llevar a cabo las funciones de gestión de usuarios.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de navegación de la aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Usuario**.
4. En la lista **Usuarios de aplicación**, seleccione el nombre de usuario.
5. Modifique la información de usuario según sea necesario
6. Pulse **Guardar**.

Cambio de una contraseña de usuario

Utilice el Asistente de integración empresarial (EIW) que el Modelador de contexto empresarial proporciona para cambiar la contraseña de usuario. La contraseña cambiada debe cumplir la política de contraseña que proporciona IBM Data Risk Manager.

Acerca de esta tarea

Debe tener el rol de administrador de BCM para llevar a cabo las funciones de gestión de usuarios.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de navegación de la aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Usuario**.
4. En la lista **Usuarios de aplicación**, seleccione el nombre de usuario.
5. Seleccione **Cambiar contraseña**.
6. Especifique la información de contraseña en los campos **Contraseña** y **Volver a escribir contraseña**.
7. Pulse **Guardar**.

Inhabilitar una cuenta de usuario

Puede inhabilitar una cuenta de usuario para impedir que el usuario acceda a IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de navegación de la aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Usuario**.
4. En la lista **Usuarios de aplicación**, seleccione la cuenta de usuario que desea inhabilitar.

5. Inhabilite el conmutador **Habilitar usuario**.
6. Pulse **Guardar**.

Desbloqueo de una cuenta de usuario
El administrador puede desbloquear una cuenta de usuario bloqueada cuando se ha excedido el número de intentos de inicio de sesión permitidos. Cuando se supera el número establecido de intentos permitidos con la contraseña incorrecta, la cuenta de bloquea.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de navegación de la aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Usuario**.
4. En la lista **Usuarios de aplicación**, seleccione la cuenta de usuario que desea desbloquear.
5. Inhabilite el conmutador **Cuenta bloqueada**.
6. Pulse **Guardar**.

Gestión de grupos de usuarios

Un grupo de usuarios es un conjunto de usuarios. Para obtener más eficiencia, considere la posibilidad de crear un grupo que contenga usuarios que realicen una tarea similar. Puede crear grupos de usuarios y asignar personas a los grupos de usuarios en IBM Data Risk Manager.

El componente Modelador de contexto empresarial de IBM Data Risk Manager proporciona el Asistente de integración empresarial (EIW) para crear los grupos de usuarios. Para crear los grupos de usuarios, se utilizan los métodos siguientes.

- Creación de un grupo de usuarios añadiendo usuarios de IBM Data Risk Manager.
- Importación de usuarios que se crean en el servidor LDAP (Lightweight Directory Access Protocol) en IBM Data Risk Manager. La importación en IBM Data Risk Manager es útil para mantener grupos de usuarios grandes.

Creación de un grupo de usuarios
Los usuarios se pueden combinar en grupos de usuarios para simplificar la administración en IBM Data Risk Manager.

Antes de empezar

Debe tener el rol de administrador de BCM para llevar a cabo las funciones de gestión de usuarios.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de navegación de la aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Grupo de usuarios**.
4. Para crear un grupo de usuarios, pulse el icono **Añadir grupo de usuarios**  .
5. Establezca las opciones siguientes y pulse **Guardar**.

Opción	Descripción
Nombre de grupo	Especifique el nombre del grupo de usuarios.
Añadir miembros	a. Para añadir un miembro al grupo de usuarios, pulse el icono **Añadir miembros**  .

Opción	Descripción
	b. Seleccione los miembros de la lista.
Miembros del grupo	Se visualizan los miembros seleccionados del grupo.

Integración de LDAP con IBM Data Risk Manager
La integración SSO-LDAP está destinada a la gestión de identidad centralizada y al inicio de sesión único, en el que los usuarios pueden iniciar sesión con sus credenciales AD/LDAP. Puede importar los grupos de usuarios a IBM Data Risk Manager y asignar roles específicos al usuario que realizar las tareas adecuadas en IBM Data Risk Manager.

IBM Data Risk Manager utiliza el microservicio para habilitar el inicio de sesión único e importar los grupos de usuarios desde los servidores de Active Directory (AD).

```
Agente de identidad (Consumo de grupos de usuarios) – se ejecuta en el puerto 8765
```

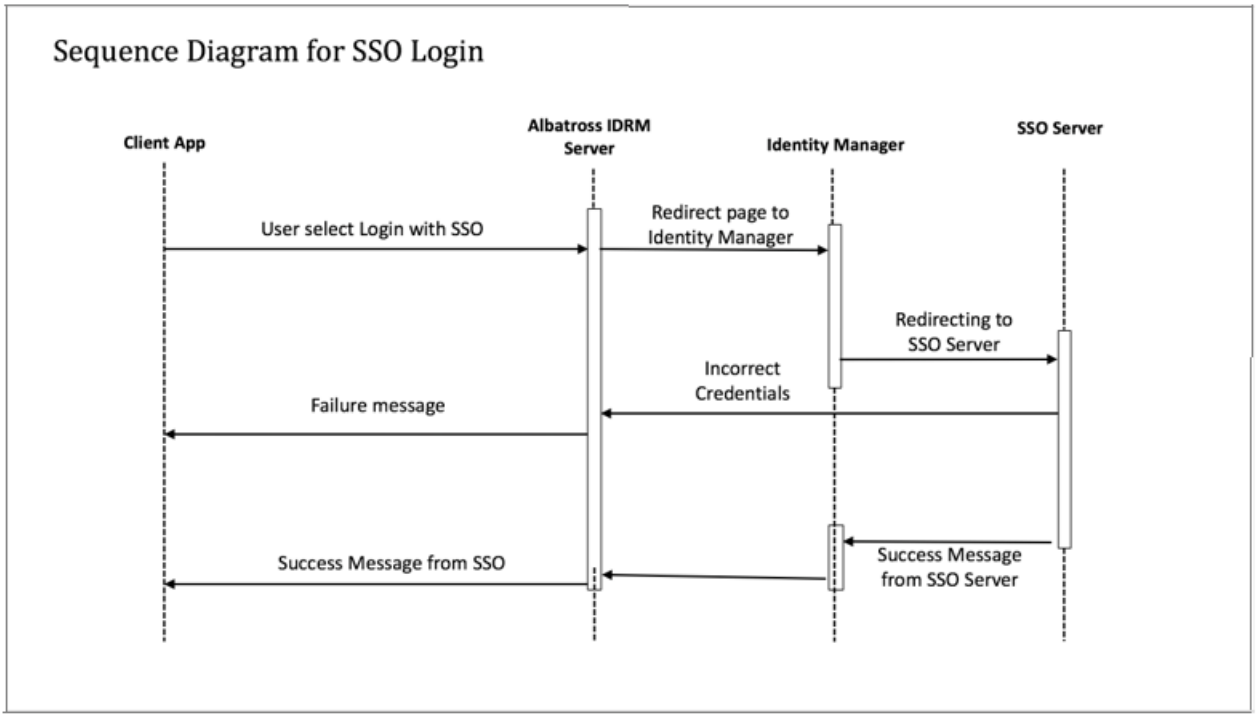
Para obtener más información sobre los requisitos previos, consulte “Requisitos previos de instalación” en la página 18.

Asegúrese de que tiene la imagen de IBM Data Risk Manager Server o que el build está disponible en el formato necesario, en función del entorno en el que está ejecutando la instalación.

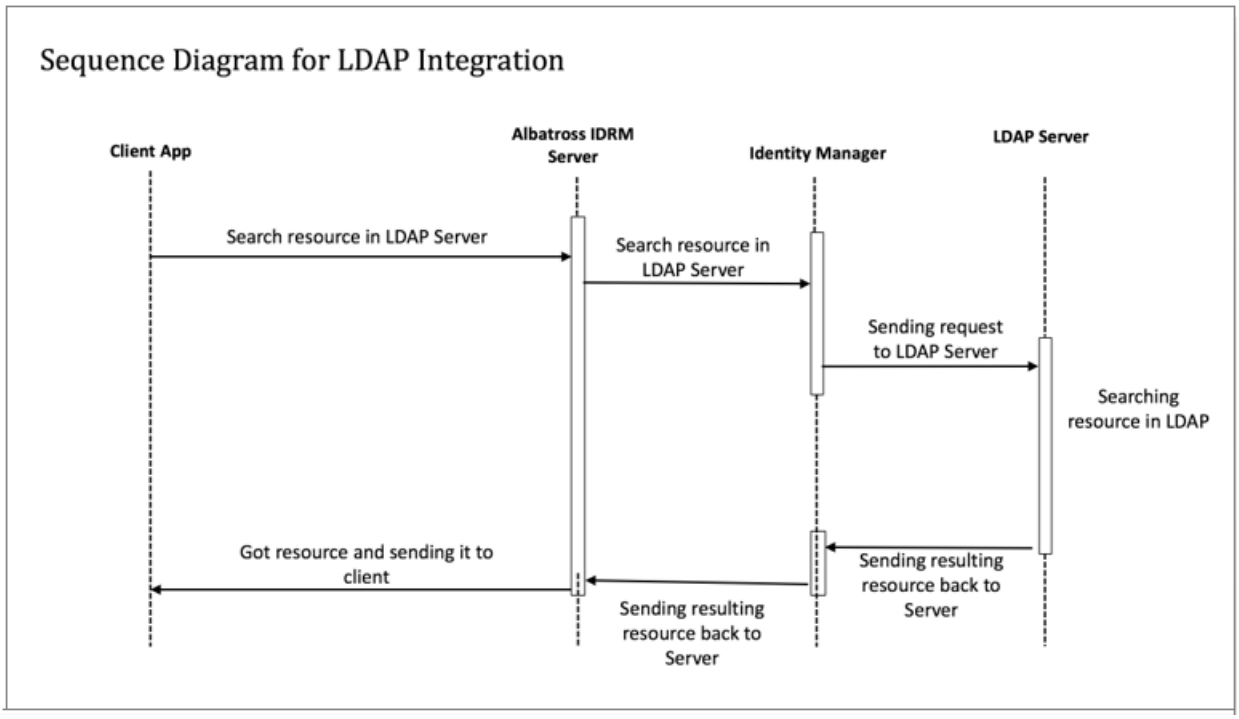
Puede configurar IBM Data Risk Manager para establecer una conexión con un directorio LDAP o un servicio SSO.

- El directorio LDAP o el servicio SSO deben estar en ejecución en un host que sea accesible para el servidor de IBM Data Risk Manager.
- Para la integración de LDAP, debe estar disponible una cuenta LDAP con nombres de usuarios y contraseñas conocidos para que los utilice IBM Data Risk Manager.
- Asegúrese de que está disponible el FQDN (Fully Qualified Domain Name) del servidor LDAP.
- Asegúrese de que esté libre el puerto en el que IBM Data Risk Manager se comunica con el servidor LDAP. El número de puerto predeterminado es 389.
- Para SSO, debe proporcionar el archivo XML IDP o el URL del servicio SSO.
- Para cualquier certificado autofirmado asociado al archivo IDP, debe proporcionar la clave de certificado y la contraseña.

Flujo de trabajo de la integración SSO en IBM Data Risk Manager



Flujo de trabajo de la integración LDAP en IBM Data Risk Manager



Integración de LDAP con IBM Data Risk Manager

Integre IBM Data Risk Manager con un servidor Lightweight Directory Access Protocol (LDAP) para importar los grupos de usuarios creados dicho servidor LDAP. La importación de grupos de usuarios en IBM Data Risk Manager es útil para mantener grupos de usuarios grandes.

Antes de empezar

Para obtener la información de requisito previo, consulte "Integración de LDAP con IBM Data Risk Manager" en la página 100.

Acerca de esta tarea

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Pulse **Administración**.
4. Pulse **Configuración del servidor** > **Configuración de inicio de sesión único y LDAP**.
5. Seleccione el microservicio de la lista.
6. Configure el inicio de sesión único (SSO).
   a) Seleccione **Habilitar SSO**.
   b) Especifique el URL de inicio de sesión SSO en **URL de inicio de sesión SSO**.
   c) Seleccione el tipo de configuración de IDP, tal como `Archivo` o URL.
      - Si selecciona `Archivo`, pulse **Elegir archivo** para localizar y cargar el archivo de configuración IDP.
      - Si selecciona URL, especifique el URL en **Especificar URL XML de IDP**.
   d) Pulse **Guardar configuración**.
7. Configure LDAP.
   a) Seleccione **Habilitar LDAP**.
   b) Seleccione el tipo de autenticación `Simple` en **Tipo de autenticación de LDAP**.
   c) Especifique el URL del proveedor LDAP en **URL del proveedor**. Por ejemplo, `ldaps://ejemplo.com:636`.
   d) Especifique el componente de dominio de los grupos de usuarios en **Componente de dominio de grupos de usuarios**. Por ejemplo, `ou=bluepages,o=ibm.com`.
   e) Especifique el componente de dominio de los usuarios en **Componente de dominio de usuarios**. Por ejemplo, `ou=bluepages,o=ibm.com`.
   f) Especifique el nombre del atributo que almacena el nombre de usuario en el servidor LDAP en **Atributo de nombre de usuario de inicio de sesión en LDAP**. Por ejemplo, `uid`.
   g) Especifique el patrón del nombre de usuario de inicio de sesión en **Patrón de nombre de usuario de inicio de sesión en LDAP**. Por ejemplo, `uid={0}, ou=bluepages, ou=in, ou=ibm`
   h) Especifique el atributo de nombre de usuario de inicio de sesión de IBM Data Risk Manager en **Atributo de nombre de usuario de IBM Data Risk Manager**. Por ejemplo, `email`.
   i) Especifique el atributo de nombre de usuario de base de datos en **Atributo de nombre de usuario de base de datos**.
   j) Para especificar el nombre de usuario y la contraseña de la cuenta del administrador de LDAP, seleccione **Credenciales de administración**.
      1) Especifique el nombre de usuario en **Nombre de usuario LDAP**.
      2) Especifique la contraseña del nombre de usuario en **Contraseña de LDAP**.
   k) Para especificar la información de inicio de sesión, seleccione **Inicio de sesión de grupo**.
      1) Especifique el atributo que contiene el nombre del grupo, tal como se define en el directorio LDAP en el **Atributo de nombre de grupo**. Por ejemplo, `cn={gName}`.

2) Especifique el atributo de nombre de usuario de grupo en **Atributo de nombre de usuario de grupo**. Por ejemplo, `uid`.
3) Especifique el atributo que contiene un usuario en un grupo, tal como se define en el directorio LDAP en el **Atributo de miembro de grupo**. Por ejemplo, `uniqueMember`.
4) Especifique el DN base de la lista de grupos en **DN base de lista de grupos**. Por ejemplo, `ou=memberlist,ou=ibmgroups`.

l) Seleccione **Campos DN base de usuario** para configurar el nombre distinguido base (DN base) con el que empezar la búsqueda en LDAP.

Un grupo dinámico define sus miembros mediante una búsqueda LDAP. Si se selecciona **DN base de usuario dinámico**, hay que especificar el valor en **Patrón de DN base de usuario**. Por ejemplo, `uid={0}, c={1}, ou={2}`.

Un grupo estático define sus miembros listándolos individualmente. Si se selecciona **DN base de usuario estático**, hay que especificar el valor en **DN base de usuario**.

m) Pulse **Guardar configuración**.

Ejemplo de archivo de configuración de LDAP.

```
com.agile3.config.ldapProviderUrl=ldaps://ejemplo.com:636
com.agile3.config.ldapAdminUsername=admin
com.agile3.config.ldapAdminPassword=password

com.agile3.config.ldapEnabled=true
com.agile3.config.ldapLoginUsernamePattern=com.agile3.config.ldapLoginUsernameAttribute=ldapL
oginUsernameAttributeValue,userBaseDn
com.agile3.config.userBaseDnPattern=c={0},ou={1},o={2}
com.agile3.config.ldapUserDomain=ou\=bluepages,o\=ibm.com
com.agile3.config.uiLoginAttribute=emailAddress
com.agile3.config.ldapAuthType=simple
com.agile3.config.userBaseDn=NA
com.agile3.config.isUserBaseDnRequired=true
com.agile3.config.ldapLoginUsernameAttribute=uid
com.agile3.config.dbUsernameAttribute=emailAddress
com.agile3.config.userBaseDnAttributesType=dynamic
com.agile3.config.isAdminCredRequired=true

com.agile3.config.isGroupLoginEnabled=true
com.agile3.config.ldapDomain=ou\=ibmgroups,o\=ibm.com
com.agile3.config.groupMemberAttribute=uniqueMember
com.agile3.config.groupListBaseDn=ou=memberlist,ou=ibmgroups,o=ibm.com
com.agile3.config.groupUsernameAttribute=uid
com.agile3.config.groupNameAttribute=cn
```

Importación de un grupo de usuarios

Puede importar usuarios que se crean en el servidor LDAP (Lightweight Directory Access Protocol) en IBM Data Risk Manager. La importación en IBM Data Risk Manager es útil para mantener grupos de usuarios grandes.

Antes de empezar

Debe tener el rol de administrador de BCM para llevar a cabo las funciones de gestión de usuarios.

Debe configurar la información de servidor LDAP utilizando el componente IBM Data Risk Manager Administration. Para obtener información de configuración de LDAP, consulte "Integración de LDAP con IBM Data Risk Manager" en la página 101.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de navegación de la aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Grupo de usuarios**.

4. Para importar un grupo de usuarios, pulse el icono **Importar grupo**  .
5. Seleccione el agente de la lista para conectarse al servidor LDAP.
6. Seleccione el grupo de usuarios de la lista que desea importar.
7. Pulse **Guardar**.

Descubrimiento de orígenes de datos nativos

Mediante el uso del programa de utilidad Network Mapper (NMAP), puede ejecutar una exploración de puerto en un rango de IP para descubrir orígenes de datos nativos o los hosts en un segmento de red. También puede definir orígenes de datos importando archivos en un formato de valor separado por coma (CSV) que contiene el inventario de orígenes de datos.

Utilice el Asistente de integración empresarial (EIW) de IBM Data Risk Manager para descubrir orígenes de datos nativos.

Ejecución de exploración de puertos para descubrir orígenes de datos

Ejecute la exploración de puertos utilizando Network Mapper (NMAP) en el rango de direcciones IP especificado para descubrir los orígenes de datos o los hosts en la red de destino.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Descubrimiento nativo**.
4. Establezca las opciones siguientes en la página **Exploración de orígenes de datos nativos con Nmap**.

Opción	Descripción
IP individual	Especifique una dirección IP para explorar un solo puerto.
Rango de IP	Especifique el rango de direcciones IP para la exploración.
Número de puerto	Especifique un número de puerto o un rango de puertos para la exploración.

5. Pulse **Explorar** para desencadenar una exploración de puertos en el rango de IP y puerto de destino.
6. Pulse **Historia** para ver y realizar el seguimiento del estado de exploración en la ventana **Exploraciones**.
7. Cuando se completa la exploración, seleccione un elemento de exploración completado en la ventana **Exploraciones**. En la página **Exploraciones IP** se listan los posibles orígenes de datos en el rango de puertos explorados.

Qué hacer a continuación

Puede añadir un origen de datos al repositorio de orígenes de datos descubiertos. Para obtener más información sobre cómo añadir un origen de datos, consulte “Adición de un origen de datos” en la página 104.

Adición de un origen de datos

Puede añadir un origen de datos al inventario de IBM Data Risk Manager para los orígenes de datos descubiertos cuando se ejecutó la exploración de puertos.

Procedimiento

1. Ejecute la exploración de puertos.

   Para ver los pasos sobre cómo ejecutar una exploración de puertos, consulte “Ejecución de exploración de puertos para descubrir orígenes de datos ” en la página 104.
2. Cuando se haya completado la exploración, seleccione el elemento de exploración completado en la página **Exploraciones**. En la página **Exploraciones IP** se listan los orígenes de datos asociados en el rango de puertos explorados.
3. En la página **Exploraciones IP**, pulse la dirección IP explorada. Se listan los orígenes de datos asociados en el rango de puertos explorados.
4. Para añadir un origen de datos, pulse el icono **Añadir origen de datos** +.
5. Establezca las opciones siguientes y pulse **Añadir**.

Opción	Descripción
Adaptador	Nombre del recopilador de datos.
Agentes	Nombre de agente para conectarse a la base de datos.
Nombre de base de datos	Nombre de la base de datos.
Identificador	Nombre del origen de datos.
Nombre de usuario	Nombre del usuario de base de datos.
Contraseña	Contraseña para el nombre de usuario de base de datos.

6. Para ver los orígenes de datos que ha añadido, pulse **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.

Importación de orígenes de datos en IBM Data Risk Manager desde un archivo CSV

Puede añadir orígenes de datos a un inventario de IBM Data Risk Manager para el descubrimiento, la clasificación y otras finalidades importando un archivo de valores separados por comas (CSV) que contiene información de origen de datos.

Acerca de esta tarea

Un archivo CSV es un archivo de datos que consta de campos y registros que se almacenan como texto. En el cual, los archivos se separan entre sí mediante comas. Si los datos de un campo contienen una coma, el campo está entre comillas. La primera línea del archivo puede contener los nombres descriptivos de las variables (columnas). Puede incluir estos títulos de columna, `Nombre de origen de datos`, `Dirección IP`, `Número de puerto`, `Tipo de base de datos`, `Nombre de base de datos`, `Suprimir`, tal como se muestra en el ejemplo siguiente.

Nombre de origen de datos	Dirección IP	Puerto	Tipo de base de datos	Nombre de base de datos	Suprimir
Oracle en 45 DS	X.XXX.XXX.XX	1521	Oracle	ORCL	FALSE
MySQL en Aceva D	X.XXX.XXX.XX	3306	MYSQL	Northwind	FALSE

Donde

Nombre de origen de datos
Identificador para distinguir de forma exclusiva la base de datos.

Dirección IP
Dirección IP del servidor o instancia de base de datos.

Puerto
Número de puerto para conectarse a la base de datos.

Tipo de base de datos
Tipo de base de datos como, por ejemplo, Oracle, MSSQL, Db2, Sybase, PostgreSQL o MySQL.

Nombre de base de datos
Nombre de la base de datos.

Suprimir
Toma como valor predeterminado FALSE para la creación del origen de datos. Si el valor se establece en TRUE, el origen de datos se suprime del servidor de IBM Data Risk Manager después de la operación de importación.

Con la información necesaria para cada base de datos de destino, se puede utilizar la plantilla de importación de definición de origen de datos de IBM Data Risk Manager para definir orígenes de datos.

Procedimiento

1. Defina información de origen de datos en el archivo de plantilla CSV.
2. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
3. Pulse el icono de menú de aplicación  .
4. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Descubrimiento nativo**.
5. Pulse **Importar**.
6. Para localizar y seleccionar el archivo CSV de definiciones de origen de datos, pulse **Seleccionar archivo**.
7. Pulse **Cargar**. Se mostrarán los orígenes de datos en la sección **Importar origen de datos**.

   Si se encuentra un error, tendrá que revisar el archivo CSV para corregir errores y volver a importar el archivo. Si la lista de orígenes de datos está estructurada de forma incorrecta o la lista de orígenes de datos contiene información incorrecta, la importación del archivo CSV podría fallar.
8. Especifique los parámetros de conexión con los orígenes de datos que se importan para establecer la conexión con la base de datos.
   a. Seleccione una base de datos y efectúe una doble pulsación.
   b. Establezca las opciones siguientes y pulse **Añadir**.

Adaptador	Nombre del recopilador de datos.
Agentes	Nombre de agente para conectarse a la base de datos.
Nombre de base de datos	Nombre de la base de datos.
Identificador	Nombre del origen de datos.
Nombre de usuario	Nombre del usuario de base de datos.
Contraseña	Contraseña para el nombre de usuario de base de datos.

9. Para ver los orígenes de datos que ha añadido, pulse **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.

Correlación de datos de contexto empresarial

IBM Data Risk Manager proporciona visibilidad de riesgos de activos de información en los datos de contexto empresarial de una organización. Para obtener esta visibilidad, es necesario comprender los

procesos de negocio, las aplicaciones, activos de datos y tener acceso a información vital y otras entidades de negocio.

Normalmente, los datos de contexto empresarial de una organización se almacenan en una base de datos de gestión de configuración (CMDB), por ejemplo, ServiceNow. De forma alternativa, los datos también se pueden adquirir a través de cuestionarios, entrevistas y talleres con las partes interesadas de cliente clave.

Importación de datos de contexto empresarial mediante archivos CSV

La visualización de riesgos de los activos de información requiere una captura e importación única inicial de los datos de contexto empresarial de la organización en lo que se refiere a unidades de negocio, líneas de negocio (LOB), procesos empresariales, aplicaciones y partes interesadas. Puede importar los datos de contexto empresarial en IBM Data Risk Manager utilizando uno o varios archivos en formato de valores separados por comas (CSV). Los metadatos de la organización se correlacionan con el metamodelo de IBM Data Risk Manager y, a continuación, se pueden configurar las vistas de panel de control para el análisis de riesgos.

Cuando se completa la correlación de contexto empresarial, los datos de contexto de la organización se pueden importar en el sistema basándose en las correlaciones completadas. Si la correlación se actualiza, los datos de contexto de la organización se deben volver a importar para mantener la integridad de los datos.

La correlación de contexto empresarial consta de los pasos siguientes.

1. Preparación de los datos de contexto empresarial para la importación.
2. Carga de los datos de contexto empresarial para la correlación.
3. Correlación de los datos de contexto empresarial.
4. Configuración de las vistas de IBM Data Risk Manager.
5. Almacenamiento del contenido y el formato estructural en el servidor de IBM Data Risk Manager.

Si desea volver a importar los datos de contexto donde solo se actualizan los datos de los archivos CSV sin ninguna columna adicional, ejecute los pasos siguientes.

1. Preparación de los datos de contexto empresarial para la importación.
2. Carga de los datos de contexto empresarial para la correlación.
3. Almacenamiento del contenido y el formato estructural en el servidor de IBM Data Risk Manager.

Visualización y gestión de datos de contexto empresarial

Puede utilizar el componente **Gestionar inventario** para ver y gestionar fácil y rápidamente aplicaciones y procesos empresariales que ha importado a través de archivos CSV como datos de contexto y sus asociaciones con otras entidades de negocio. Para obtener más información sobre cómo gestionar los datos de contexto, consulte “Inventario de aplicaciones ” en la página 126 y “Inventario de procesos de negocio ” en la página 129.

Importar CMDB de ServiceNow a IBM Data Risk Manager

Puede configurar ServiceNow para importar los datos de CMDB (Configuration Management Database) en IBM Data Risk Manager y utilizar estos datos junto con las aplicaciones y el contexto empresarial.

Para obtener más información sobre cómo importar CMDB de ServiceNow en IBM Data Risk Manager, consulte “Integración de ServiceNow con IBM Data Risk Manager” en la página 74.

Preparación de datos de contexto empresarial para la importación.

Para correlacionar los datos de contexto empresarial, debe capturar o preparar los datos de contexto para importarlos en IBM Data Risk Manager.

Acerca de esta tarea

En una organización, la información de contexto empresarial se puede encontrar en un tipo de sistemas CMDB (Configuration Management Database) o en hojas de trabajo que mantienen los equipos de gestión de bases de datos. Las organizaciones pueden tener un inventario de aplicaciones que se mantiene manualmente o en aplicaciones de arquitectura de empresa que contienen información sobre los procesos empresariales asociados, departamentos, partes interesadas u otros metadatos relevantes. Si la información de contexto empresarial no está disponible, los datos se pueden capturar mediante encuestas y sesiones de recopilación de información que se llevan a cabo con las partes interesadas de la organización.

Se pueden importar las categorías de conjuntos de datos de contexto de organización siguientes en IBM Data Risk Manager.

- Base de datos
- Aplicación
- Proceso empresarial

Los conjuntos de datos asociados a las tres categorías se pueden capturar en un único archivo CSV o en varios. Debe existir un campo común (campo de enlace) para enlazar juntos los tres conjuntos de datos. Por ejemplo, un identificador de aplicación puede ser el campo de enlace. La aplicación es la entidad en la mayoría de las organizaciones que enlazan los procesos empresariales y otros metadatos empresariales con los repositorios de datos en los que se almacenan los datos.

Procedimiento

Prepare el contenido de los archivos CSV para las categorías de Base de datos, Aplicación y Proceso empresarial que son relevantes para la organización.

Qué hacer a continuación

Cargue los metadatos de contexto empresarial. Para obtener más información sobre cómo cargar los conjuntos de datos, consulte “Carga de datos de contexto empresarial” en la página 108.

Carga de datos de contexto empresarial

Debe cargar los datos de contexto empresarial para la correlación con el glosario de metadatos de IBM Data Risk Manager.

Antes de empezar

Asegúrese de que los datos de contexto empresarial están disponibles para cargarse. Para obtener más información sobre la preparación de los datos de contexto, consulte “Preparación de datos de contexto empresarial para la importación.” en la página 108.

Puede descargar las plantillas de ejemplo en: http://www.ibm.com/support/docview.wss?uid=ibm10731739

El número de columnas en los archivos CSV de datos de contexto que importa a IBM Data Risk Manager no debe exceder los 49.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).

2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización** > **Cargar contexto empresarial**.
4. Para seleccionar archivos de datos, seleccione **Cargar archivos de configuración y de datos**.
   a) Pulse el icono de archivo CSV para seleccionar los archivos CSV de `Base de datos`, `Aplicación` y `Proceso empresarial`.

   Seleccione **Cargar archivos de datos** para cargar archivos en los que los datos se actualizan sin ninguna columna adicional en los archivos CSV que ya se han importado.
5. Pulse **Siguiente**.

Qué hacer a continuación

Correlacionar los datos de contexto empresarial con el glosario de metadatos de IBM Data Risk Manager para especificar la taxonomía empresarial de los activos de información descubiertos. Para obtener más información sobre cómo correlacionar los datos de contexto, consulte "Correlación de datos de contexto empresarial" en la página 109.

Correlación de datos de contexto empresarial

Debe correlacionar los datos de contexto empresarial con el glosario de metadatos de IBM Data Risk Manager para especificar la taxonomía empresarial de los activos de información descubiertos.

Antes de empezar

Asegúrese de que los datos de contexto empresarial se cargan en IBM Data Risk Manager. Para obtener más información sobre cómo cargar los datos de contexto empresarial, consulte "Carga de datos de contexto empresarial" en la página 108.

Acerca de esta tarea

La correlación de datos de contexto es una actividad única y un paso de requisito previo para importar los datos. La correlación de atributos con el glosario empresarial de IBM Data Risk Manager se puede actualizar en cualquier momento. Sin embargo, cualquier cambio en la correlación debe ir seguido de la importación de los datos de contexto para garantizar la correlación completa.

Se debe seleccionar un atributo entre los metadatos de `Base de datos`, `Aplicación` y `Proceso empresarial` como campo común o como `Campo de enlace` para correlacionar los atributos entre las tres entidades diferentes.

De forma predeterminada, todos los atributos de entidad de contexto empresarial se marcan como `Propiedad`, que es un atributo de propósito general. Aparte de este atributo, el Modelador de contexto empresarial identifica las cuatro categorías siguientes de atributos.

Resolución de BD

Representa los datos específicos de la infraestructura de datos de la organización. Los datos incluyen atributos que ayudan a identificar la información de base de datos para la ingesta en IBM Data Risk Manager. Los atributos siguientes son necesarios para la resolución de base de datos y se listan como tipo de subpropiedad.

- Nombre de base de datos
- Dirección IP
- Servidor
- Nombre
- Tipo de base de datos

Titularidades

Representa los metadatos que se pueden utilizar para definir el ámbito para el descubrimiento y la clasificación de datos. Por ejemplo, `Entorno` es una propiedad de titularidad que se puede utilizar

para crear el ámbito del descubrimiento de datos que se ejecutará en bases de datos de producción, prueba o desarrollo. Los siguientes atributos de titularidad se definen en el metamodelo de IBM Data Risk Manager.

- Conformidad
- Entorno
- Línea de negocio

Correlación de taxonomía
Representa los datos específicos de la visualización del contexto empresarial en IBM Data Risk Manager. Estos atributos se utilizan durante la definición y asignación de taxonomías. Los siguientes atributos de correlación de taxonomías se definen en el metamodelo de IBM Data Risk Manager.

- Grupo: nivel de organización
- Aplicación
- Proceso de soporte de empresa
- Nivel 2 de organización consumidora
- Nivel 1 de organización consumidora

Recurso
Identifica el atributo que va a ser un rol o un recurso.

Nota: Si la información de configuración de la importación de datos de contexto anterior está disponible en el sistema, la información de correlación se restaura para los atributos similares.

Procedimiento

1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización** > **Correlacionar contexto empresarial**.
2. Para correlacionar los atributos entre las tres entidades diferentes, seleccione un campo común o un campo de enlace de la lista desplegable **Campo de enlace**. Por ejemplo, APP_ASSETID.
3. Pulse **Resolución de BD** para correlacionar los atributos de resolución de base de datos.
   a) Pulse el icono Añadir ⊕ situado junto al atributo y especifique el nombre de columna del archivo CSV en **Buscar columnas**.

      Por ejemplo, para correlacionar DB_Name con Nombre de base de datos en el archivo CSV, especifique Nombre de base de datos en **Buscar columnas**. Se mostrará y se correlacionará el nombre de columna.
   b) Correlacione los atributos restantes con las columnas correspondientes del archivo CSV.
4. Pulse **Titularidades** para correlacionar los atributos de titularidad.
   a) Pulse el icono Añadir ⊕ situado junto al atributo y especifique el nombre de columna del archivo CSV en **Buscar columnas**.

      Por ejemplo, para correlacionar Conformidad con SOX en el archivo CSV, especifique SOX en **Buscar columnas**. Se mostrará y se correlacionará el nombre de columna.
   b) Correlacione los atributos restantes con las columnas correspondientes del archivo CSV.
5. Pulse **Correlación de taxonomía** para correlacionar los atributos de taxonomía.
   a) Pulse el icono Añadir ⊕ situado junto al atributo y especifique el nombre de columna del archivo CSV en **Buscar columnas**.

      Por ejemplo, para correlacionar Nivel 1 de organización consumidora con Business_Support_Consuming_Organization_Level_1 en el archivo CSV, especifique Business_Support_Consuming_Organization_Level_1 en **Buscar columnas**. Se mostrará y se correlacionará el nombre de columna.
   b) Correlacione los atributos restantes con las columnas correspondientes del archivo CSV.

6. Pulse **Recurso** para correlacionar los atributos de titularidad.

   a) Pulse el icono Añadir  situado junto al atributo y especifique el nombre de columna del archivo CSV en **Buscar columnas**.

   Por ejemplo, para correlacionar `Propietario de producto` con `Application_Owner` en el archivo CSV, especifique `Application_Owner` en **Buscar columnas**. Se mostrará y se correlacionará el nombre de columna.

   b) Correlacione los atributos restantes con las columnas correspondientes del archivo CSV.

7. Pulse **Siguiente**.

Qué hacer a continuación

Configure el panel de control de IBM Data Risk Manager. Para obtener más información sobre cómo configurar el panel de control, consulte "Configuración del panel de control de IBM Data Risk Manager" en la página 111.

Configuración del panel de control de IBM Data Risk Manager

Debe configurar widgets del panel de control de IBM Data Risk Manager para mostrar los atributos correlacionados.

Antes de empezar

Asegúrese de que los datos de contexto empresarial se correlacionan con el glosario de metadatos de IBM Data Risk Manager. Para obtener más información sobre cómo correlacionar los datos de contexto, consulte "Correlación de datos de contexto empresarial" en la página 109.

Acerca de esta tarea

Puede configurar los atributos en los siguientes widgets del panel de control de IBM Data Risk Manager utilizando el mecanismo de arrastrar y soltar.

- Infraestructura
- Aplicación
- Proceso empresarial
- Recurso

Nota: Si la información de configuración de la importación de datos de contexto anterior está disponible en el sistema, se restaura la información de configuración del panel de control. Si es necesario, puede modificar la configuración.

Procedimiento

1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización** > **Configurar panel de control de IBM Data Risk Manager**.
2. Pulse el icono de atributo en **Propiedades asignadas** y, a continuación, arrastre el nombre de atributo correspondiente en el widget del panel de control de IBM Data Risk Manager. El nombre de atributo correlacionado se visualiza en **Atributos de Data Risk Manager**.

   Por ejemplo, pulse el icono **ENV**  en **Base de datos** > **Propiedades asignadas** y, a continuación, arrastre **Entorno** en el widget **Correlación de IDRM** > **Infraestructura**. El nombre de atributo soltado se visualiza en **Atributos de Data Risk Manager**.
3. Configure los widgets del panel de control de IBM Data Risk Manager con los atributos restantes de **Base de datos**, **Aplicación** y **Proceso empresarial**.
4. Para configurar el widget **Recurso**, los atributos que se van a arrastrar deben ser de tipo de propiedad `Recurso`. La asignación de responsabilidad de los interesados sigue la matriz RACI para los roles

clave definidos en los datos de contexto. Arrastre el icono **Recurso** sobre las secciones circulares bajo el widget **Recurso**.

5. Pulse **Siguiente**.

Qué hacer a continuación

Puede crear grupos y asignarles atributos en función de un contexto empresarial. Si desea más información, consulte "Correlación de propiedades de IBM Data Risk Manager" en la página 112.

Cuando pulsa **Siguiente**, se le solicita que guarde los valores para la correlación de atributos y la configuración del panel de control. Para continuar, pulse **Sí**. Para obtener más información sobre cómo guardar e importar los datos de contexto, consulte "Importación de datos de contexto empresarial" en la página 113.

Correlación de propiedades de IBM Data Risk Manager

Puede configurar los widgets del panel de control de IBM Data Risk Manager para visualizar los atributos, que están configurados y agrupados en función de un contexto empresarial, en una ventana emergente.

Procedimiento

1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización** > **Configurar panel de control de IBM Data Risk Manager** > **Correlación de propiedad de iDRM**.
2. Cree grupos para los atributos de las categorías **Base de datos**, **Aplicación** y **Proceso empresarial** y añada atributos al grupo.

   Ejecute los pasos siguientes para crear un grupo.

   a. Seleccione **Base de datos**, **Aplicación** o **Proceso empresarial** de acuerdo con sus requisitos.
   b. Pulse **Añadir grupo**.
   c. Especifique un nombre de grupo.
   d. Para asignar un nombre de grupo a todas las columnas sin asignar, seleccione **Asignar el grupo a las columnas sin asignar**.
   e. Pulse **Guardar**.

   Ejecute los pasos siguientes para añadir atributos a un grupo.

   a. Seleccione un grupo.
   b. Seleccione un atributo de la lista.
   c. Especifique el nombre de atributo que se va a visualizar en la ventana emergente del widget del panel de control.
   d. Para seleccionar el tipo de campo de datos que se va a visualizar para el atributo en la ventana emergente del widget, pulse el icono desplegable . Por ejemplo, campo de texto, recuadro de selección, distintivo o gráfico circular.
   e. Repita los mismos pasos para todos los atributos de acuerdo con los requisitos.
3. Para Para borrar información de correlación de propiedades, pulse el icono para borrar correlación
4. Pulse **Siguiente**.

Qué hacer a continuación

Cuando pulsa **Siguiente**, se le solicita que guarde los valores para la correlación de atributos y la configuración del panel de control. Para continuar, pulse **Sí**. Para obtener más información sobre cómo guardar e importar los datos de contexto, consulte "Importación de datos de contexto empresarial" en la página 113.

Importación de datos de contexto empresarial

Importe los datos de contexto para correlacionar los datos de contexto con el glosario empresarial de IBM Data Risk Manager y especificar los atributos relacionados con las bases de datos, las aplicaciones y los procesos empresariales.

Antes de empezar

Asegúrese de que todos los atributos están configurados en los diversos widgets del panel de control. Para obtener más información sobre cómo configurar los widgets del panel de control de IBM Data Risk Manager, consulte "Configuración del panel de control de IBM Data Risk Manager" en la página 111.

Acerca de esta tarea

Después de guardar los valores para la correlación de atributos y la configuración del panel de control, se le solicitará que importe los datos de contexto empresarial. Pulse **Sí** para continuar.

Procedimiento

1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización** > **Validar importación de contexto empresarial**.
2. Cuando se le solicite, pulse **Sí** para continuar con el guardado de los valores de configuración y la importación de datos.
3. El contenido se visualiza en formato tabular. Pulse **Guardar** para guardar la configuración.
4. Cuando se le solicite, pulse **Sí** para importar los datos de contexto. Se importarán los archivos de datos específicos de la organización y los valores de configuración en IBM Data Risk Manager.

   Nota: Si la información de correlación no es correcta, se muestra una hoja de resumen de correlación para ver los datos. Debe corregir la información de correlación para continuar con la operación de importación.

Gestión de inventario

Utilice el componente Gestionar inventario para ver y gestionar elementos de inventario de IBM Data Risk Manager como, por ejemplo, orígenes de datos, aplicaciones, procesos de negocio, activos de información y amenazas.

Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** para ver y gestionar los elementos de inventario siguientes.

Aplicación
: Vea y gestione todas las aplicaciones en el inventario de IBM Data Risk Manager. Para obtener más información sobre cómo gestionar el inventario de aplicaciones, consulte "Inventario de aplicaciones " en la página 126.

Proceso empresarial
: Vea y gestione todos los procesos de negocio en el inventario de IBM Data Risk Manager. Para obtener más información sobre cómo gestionar el inventario de procesos de negocio, consulte "Inventario de procesos de negocio " en la página 129.

Origen de datos
: Vea y gestione todos los orígenes de datos en el inventario de IBM Data Risk Manager. Para obtener más información sobre cómo gestionar el inventario de orígenes de datos, consulte "Inventario de orígenes de datos " en la página 114.

Amenaza
: Vea y gestione todas las posibles amenazas en el inventario de IBM Data Risk Manager. Para obtener más información sobre cómo gestionar el inventario de orígenes de datos, consulte "Inventario de amenazas " en la página 131.

Inventario de orígenes de datos

Puede ver y gestionar todos los orígenes de datos que contiene el inventario de IBM Data Risk Manager desde una sola ubicación para realizar un seguimiento de la información de origen de datos.

El origen de datos puede ser un repositorio en el que se almacenan los datos de una organización. IBM Data Risk Manager admite datos estructurados como, por ejemplo, bases de datos y datos no estructurados como, por ejemplo, comparticiones de archivo. Puede definir y gestionar varios orígenes de datos en IBM Data Risk Manager.

Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** para ver y gestionar los orígenes de datos.

Visualización del inventario de orígenes de datos

Puede ver y gestionar fácilmente información de origen de datos desde una única ubicación. Utilice el componente **Gestionar inventario** > **Origen de datos** para realizar un seguimiento de todos los orígenes desde los cuales se han añadido o importado datos al inventario de IBM Data Risk Manager para un descubrimiento de datos y operaciones de clasificación.

Acerca de esta tarea

Debe relacionar información de contexto empresarial que incluya aplicaciones de negocio, procesos empresariales y partes interesadas con datos confidenciales descubiertos de distintos orígenes. Para obtener más información los datos de contexto empresarial, consulte "Correlación de datos de contexto empresarial" en la página 106.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Para ver la lista de orígenes de datos de distintos orígenes y sus atributos, vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.
4. En la página **Crear/Actualizar inventario**, seleccione un tipo de origen de datos como, por ejemplo, **Base de datos**, **Almacenamiento de archivos**, **Aplicación** o **Servidor** para ver orígenes de datos asociados y sus atributos en formato tabla.
5. Para añadir un origen de datos al inventario, seleccione un tipo de origen y pulse el icono **Añadir origen de datos** .
6. Para un origen de datos seleccionado, pulse el icono **Acciones** para ejecutar las operaciones siguientes basándose en el tipo de origen de datos seleccionado.
   - Para modificar información de origen de datos, pulse el icono **Editar** .

     Nota: No puede editar detalles de los orígenes de datos del tipo **Aplicación**.
   - Para suprimir un origen de datos del inventario, pulse el icono **Suprimir** .

     Nota: Puede suprimir solo los orígenes de datos nativos de IBM Data Risk Manager y los orígenes de datos de IBM Security Guardium del inventario.
   - Puede limitar la visualización de orígenes de datos en la lista basándose en la opción de filtro que seleccione. Pulse el icono de filtro para seleccionar la opción de filtro.
7. Para un origen de datos seleccionado, también puede ver la información siguiente.

Icono	Descripción
	Indica que los datos contienen información de joya de la corona.
	Indica que los datos están clasificados.
	Indica que los datos contienen información confidencial.
	La bandera de un país indica donde reside el origen de datos.
	Indica que el origen de datos se ha correlacionado con entidades de contexto empresarial.

Adición de orígenes de datos a inventario

Puede añadir orígenes de datos al inventario de IBM Data Risk Manager desde varios orígenes para evaluar los riesgos que están asociados a los activos de datos.

Vaya a **Modelador del contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** para añadir los orígenes de datos.

Adición de un origen de datos nativo

Puede añadir un origen de datos estructurados nativos en el inventario de IBM Data Risk Manager para que sus datos estén disponibles para el análisis de riesgos y acciones.

Antes de empezar

Antes de crear un origen de datos, debe tener en cuenta los parámetros de conexión de base de datos para el origen de datos al que desee conectarse.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.
4. Para añadir un origen de datos estructurados nativos, pulse el icono **Añadir origen de datos**  .
5. En la página **Añadir origen de datos**, especifique las propiedades de base de datos para el origen de datos y pulse **Añadir**.

Opción	Descripción
Tipo de servidor	Servidor de base de datos que desea utilizar. Por ejemplo, **Oracle**. Para el servidor MSSQL, si el servidor está habilitado para utilizar la autenticación de Windows, puede conectarse a la base de datos utilizando las credenciales de inicio de sesión de usuario de Windows para la autenticación. Ejecute los pasos siguientes para la autenticación basada en Windows para servidor MSSQL. a. Seleccione **Habilitar autenticación de dominio**. b. Especifique el nombre de dominio del servidor en el campo **Nombre de dominio**.
Nombre de origen de datos	Nombre exclusivo para el origen de datos.

Opción	Descripción
Dirección IP	Dirección IP del servidor de bases de datos.
Puerto	Número de puerto de escucha del servidor de base de datos.
Nombre de base de datos	Nombre de la base de datos.
Adaptador	Nombre de instancia de adaptador. Por ejemplo, `Nativo con estructura`.
Agentes	Nombre de agente para conectarse al origen de datos.
Nombre de usuario	Nombre del usuario para conectarse al origen de datos.
Contraseña	Contraseña para el nombre de usuario de base de datos.
Cifrado	Estado de cifrado del servidor de origen de datos.
Supervisión	Estado del agente de supervisión de base de datos.
URL personalizado	Serie de URL personalizado para conectarse al origen de datos.
Ubicación geográfica	Ubicación geográfica del origen de datos.

El origen de datos que ha añadido aparece listado en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Base de datos**.

Adición de orígenes de datos no estructurados nativos

Puede añadir orígenes de datos nativos no estructurados en el inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.
4. Para añadir un origen de datos no estructurados, pulse el icono **Añadir origen de datos**  .
5. En la página **Añadir origen de datos**, establezca las opciones siguientes y pulse **Añadir**.

Opción	Descripción
Tipo de servidor	El tipo de servidor de origen de datos que desea utilizar. Por ejemplo, **IDRM**.
Destino	Nombre del origen de datos.
Dirección IP	La dirección IP del servidor de origen de datos.
Puerto	El número de puerto para conectarse al servidor de origen de datos.
Tipo de puerto	El protocolo de compartición de archivos par acceder a datos.
Vía de acceso de destino	Vía de acceso de destino para importar los datos no estructurados.
Adaptador	Nombre de instancia de adaptador. Por ejemplo, `Nativo sin estructura`.

Opción	Descripción
Agentes	Nombre de agente para conectarse al origen de datos.
Nombre de usuario	Nombre del usuario.
Contraseña	Contraseña para el nombre de usuario.
Cifrado	Estado de cifrado del servidor de origen de datos.
Supervisión	Estado del agente de supervisión.
Ubicación geográfica	Ubicación geográfica del origen de datos.

El origen de datos que ha añadido se muestra en la lista en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Almacenamiento de archivos**.

Adición de orígenes de datos de IBM Security Guardium

Puede añadir orígenes de datos de IBM Security Guardium en el inventario de IBM Data Risk Manager para que los datos estén disponibles para el análisis de riesgos y acciones.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security Guardium. Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium con IBM Data Risk Manager" en la página 38.

Antes de crear un origen de datos, debe tener en cuenta los parámetros de conexión de base de datos para el origen de datos al que desee conectarse.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.
4. Para añadir un origen de datos de IBM Security Guardium, pulse el icono **Añadir origen de datos**  .
5. En la página **Añadir origen de datos**, establezca las opciones siguientes y pulse **Añadir**.

Opción	Descripción
Tipo de servidor	El tipo de servidor de base de datos que desea utilizar. Por ejemplo, `MySQL`.
Nombre de origen de datos	Nombre exclusivo para el origen de datos.
Dirección IP	Dirección IP del servidor de bases de datos.
Puerto	Número de puerto de escucha del origen de datos.
Nombre de base de datos	Nombre de la base de datos.
Adaptador	Nombre de instancia de IBM Security Guardium. Por ejemplo, `Guardium_Adapter`.
Agentes	Nombre de agente para conectarse a la base de datos.

Opción	Descripción
Nombre de usuario	El nombre del usuario para conectarse a la base de datos.
Contraseña	Contraseña para el nombre de usuario de base de datos.
Cifrado	Estado de cifrado del servidor de origen de datos.
Supervisión	El estado del agente de supervisión de base de datos como, por ejemplo, S-TAP.
URL personalizado	Serie de URL personalizado para conectarse al origen de datos.
Ubicación geográfica	Ubicación geográfica del origen de datos.

El origen de datos que ha añadido aparece listado en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Base de datos**.

Adición de orígenes de datos de DLP de Symantec

Puede añadir orígenes de datos DLP de Symantec en el inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con DLP de Symantec. Para obtener más información sobre la integración, consulte "Integración de Symantec DLP con IBM Data Risk Manager" en la página 69.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.
4. Para añadir un origen de datos de DLP de Symantec, pulse el icono **Añadir origen de datos** .
5. En la página **Añadir origen de datos**, establezca las opciones siguientes y pulse **Añadir**.

Opción	Descripción
Tipo de servidor	El tipo de servidor de origen de datos que desea utilizar. Por ejemplo, **IDRM**.
Destino	Nombre del origen de datos.
Dirección IP	La dirección IP del servidor de origen de datos.
Puerto	Número de puerto para conectarse al servidor.
Tipo de puerto	El protocolo de compartición de archivos par acceder a datos.
Vía de acceso de destino	Vía de acceso de destino para importar los datos no estructurados.
Adaptador	Nombre de instancia de DLP de Symantec. Por ejemplo, `Instancia de DLP de Symantec`.
Agentes	Nombre de agente para conectarse al origen de datos.

Opción	Descripción
Nombre de usuario	Nombre del usuario.
Contraseña	Contraseña para el nombre de usuario.
Cifrado	Estado de cifrado del servidor de origen de datos.
Supervisión	Estado del servidor de origen de datos de agente de supervisión.
Ubicación geográfica	Ubicación geográfica del origen de datos.

El origen de datos que ha añadido se muestra en la lista en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Almacenamiento de archivos**.

Adición de orígenes de datos de IBM Security AppScan Enterprise

Puede añadir orígenes de datos de IBM Security AppScan Enterprise en el inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security AppScan Enterprise. Para obtener más información sobre la integración, consulte "Integración de IBM Security AppScan Enterprise con IBM Data Risk Manager" en la página 62.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.
4. Para añadir un origen de datos de IBM Security AppScan Enterprise, pulse el icono **Añadir origen de datos**  .
5. En la página **Añadir origen de datos**, establezca las opciones siguientes y pulse **Añadir**.

Opción	Descripción
Tipo de servidor	El tipo de servidor que desea utilizar. Por ejemplo, **IBM Appscan**.
Nombre de origen de datos	Nombre exclusivo para el origen de datos.
URL de host	El URL del servidor de host para importar datos.
Dirección IP	Dirección IP del servidor.
Puerto	Número de puerto para conectarse al servidor.
Adaptador	Nombre de instancia de IBM Security AppScan Enterprise. Por ejemplo, `AppScan_Instance`.
Agentes	El nombre de agente para conectarse al servidor.
Nombre de usuario	El nombre del usuario para conectarse al servidor.

Opción	Descripción
Contraseña	Contraseña para el nombre de usuario.
Cifrado	Estado de cifrado del servidor de origen de datos.
Supervisión	Estado del agente de supervisión.
Ubicación geográfica	Ubicación geográfica del origen de datos.

El origen de datos que ha añadido aparece listado en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Aplicación**.

Adición de orígenes de datos de IBM QRadar Security Intelligence Platform
Puede añadir orígenes de datos IBM QRadar Security Intelligence Platform en el inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con IBM QRadar Security Intelligence Platform. Para obtener más información sobre la integración, consulte IntegraciónIBM QRadar Security Intelligence Platform con IBM Data Risk Manager.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.
4. Para añadir un origen de datos de IBM QRadar Security Intelligence Platform, pulse el icono **Añadir origen de datos** .
5. En la página **Añadir origen de datos**, establezca las opciones siguientes y pulse **Añadir**.

Opción	Descripción
Tipo de servidor	El tipo de servidor de origen de datos que desea utilizar, por ejemplo, `Servidor`.
Nombre de origen de datos	Nombre del origen de datos.
Dirección IP	La dirección IP del servidor de origen de datos.
Adaptador	Nombre de instancia de IBM QRadar Security Intelligence Platform. Por ejemplo, `Qradar_Adapter`.
Agentes	Nombre de agente para conectarse al origen de datos.
Nombre de usuario	Nombre del usuario.
Contraseña	Contraseña para el nombre de usuario.
Cifrado	Estado de cifrado del servidor de origen de datos.
Supervisión	Estado del agente de supervisión.
Ubicación geográfica	Ubicación geográfica del origen de datos.

El origen de datos que ha añadido aparece en la lista en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Servidor**.

Importación de orígenes de datos al inventario

Puede importar orígenes de datos al inventario de IBM Data Risk Manager de varios orígenes para evaluar los riesgos que están asociados a los activos de datos.

Importación de orígenes de datos de IBM Security Guardium

Puede importar orígenes de datos desde dispositivos IBM Security Guardium en el inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security Guardium. Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium con IBM Data Risk Manager" en la página 38.

Acerca de esta tarea

El icono de transacción  indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción  indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Origen de datos**.
4. Importe orígenes de datos.
   a) Pulse el icono **Descargar**  .
   b) En la ventana **Importar**, seleccione una instancia de adaptador IBM Security Guardium.
   c) Pulse **Importar**.
      Cuando se haya completado la operación de importación, se añadirán los orígenes de datos de IBM Security Guardium al inventario.
   d) Para renovar la lista de inventario de orígenes de datos, pulse el icono **Renovar**  .

   El origen de datos que ha añadido aparece listado en la página **Origen de datos**. De forma alternativa, también puede ver los orígenes de datos que ha importado en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración de empresarial** > **Gestionar inventario** > **Origen de datos** > **Base de datos**.

Importación de orígenes de datos de IBM Security AppScan Enterprise

Puede importar orígenes de datos de IBM Security AppScan Enterprise al inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security AppScan Enterprise. Para obtener más información sobre los pasos de integración, consulte "Integración de IBM Security AppScan Enterprise con IBM Data Risk Manager" en la página 62.

Acerca de esta tarea

El icono de transacción  indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción  indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Origen de datos**.
4. Importe orígenes de datos.

   a) Pulse el icono **Descargar**  .

   b) En la ventana **Importar**, seleccione una instancia de IBM Security AppScan Enterprise en la lista.

   c) Pulse **Importar**.

   Cuando se haya completado la operación de importación, se añadirán los orígenes de datos de IBM Security AppScan Enterprise al inventario.

   d) Para renovar la lista de inventario de orígenes de datos, pulse el icono **Renovar**  .

   El origen de datos que ha añadido aparece listado en la página **Origen de datos**. De forma alternativa, también puede ver los orígenes de datos que ha importado en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Aplicación**.

Importación de orígenes de datos de IBM QRadar Security Intelligence Platform
Se pueden importar los orígenes de datos de IBM QRadar Security Intelligence Platform en el inventario de IBM Data Risk Manager para clasificar datos y analizar riesgos.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con IBM QRadar Security Intelligence Platform. Para obtener más información sobre los pasos de integración, consulte "Integración de IBM QRadar Security Intelligence Platform con IBM Data Risk Manager" en la página 54.

Acerca de esta tarea

El icono de transacción  indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción  indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Origen de datos**.
4. Importe orígenes de datos.

a) Pulse el icono **Descargar**  .

b) En la ventana **Importar**, seleccione una instancia de IBM QRadar Security Intelligence Platform en la lista.

c) Pulse en la pestaña **Importar**.

Cuando se haya completado la operación de importación, se añadirán los orígenes de datos de IBM QRadar Security Intelligence Platform al inventario.

d) Para renovar la lista de inventario de orígenes de datos, pulse el icono **Renovar**  .

El origen de datos que ha añadido aparece listado en la página **Origen de datos**. De forma alternativa, también puede ver los orígenes de datos que ha importado en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Servidor**.

Importación de orígenes de datos de IBM Security Guardium Analyzer

Puede importar orígenes de datos de IBM Security Guardium Analyzer al inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security Guardium Analyzer. Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium Analyzer con IBM Data Risk Manager" en la página 88.

Acerca de esta tarea

El icono de transacción  indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción  indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Origen de datos**.
4. Importe orígenes de datos.

a) Pulse el icono **Descargar**  .

b) En la ventana **Importar**, seleccione una instancia de IBM Security Guardium Analyzer.

c) Pulse **Importar**.

Cuando se haya completado la operación de importación, se añadirán los orígenes de datos de IBM Security Guardium Analyzer al inventario.

d) Para renovar la lista de inventario de orígenes de datos, pulse el icono **Renovar**  .

El origen de datos que ha añadido aparece listado en la página **Origen de datos**. De forma alternativa, también puede ver los orígenes de datos que ha importado en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración de empresarial** > **Gestionar inventario** > **Origen de datos** > **Base de datos**.

Importación de orígenes de datos de IBM StoredIQ

Puede importar orígenes de datos no estructurados desde IBM StoredIQ al inventario de IBM Data Risk Manager para el análisis de riesgos y acciones.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM StoredIQ. Para obtener más información sobre la integración, consulte "Integración de IBM StoredIQ con IBM Data Risk Manager" en la página 92.

Acerca de esta tarea

El icono de transacción  indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción  indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Origen de datos**.
4. Importe orígenes de datos.
   a) Pulse el icono **Descargar**  .
   b) En la ventana **Importar**, seleccione una instancia de IBM StoredIQ.
   c) Pulse **Importar**.
      Cuando se haya completado la operación de importación, se añadirán los orígenes de datos de IBM StoredIQ al inventario.
   d) Para renovar la lista de inventario de orígenes de datos, pulse el icono **Renovar**  .

   El origen de datos que ha añadido aparece listado en la página **Origen de datos**. De forma alternativa, también puede ver los orígenes de datos que ha importado en la página **Crear/Actualizar inventario** en **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos** > **Almacenamiento de archivos**.

Importación de orígenes de datos en IBM Data Risk Manager desde un archivo CSV

Puede añadir orígenes de datos a un inventario de IBM Data Risk Manager para el descubrimiento, la clasificación y otras finalidades importando un archivo de valores separados por comas (CSV) que contiene información de origen de datos.

Acerca de esta tarea

Un archivo CSV es un archivo de datos que consta de campos y registros que se almacenan como texto. En el cual, los archivos se separan entre sí mediante comas. Si los datos de un campo contienen una coma, el campo está entre comillas. La primera línea del archivo puede contener los nombres descriptivos de las variables (columnas). Puede incluir estos títulos de columna, `Nombre de origen de datos`, `Dirección IP`, `Número de puerto`, `Tipo de base de datos`, `Nombre de base de datos`, `Suprimir`, tal como se muestra en el ejemplo siguiente.

Nombre de origen de datos	Dirección IP	Puerto	Tipo de base de datos	Nombre de base de datos	Suprimir
Oracle en 45 DS	X.XXX.XXX.XX	1521	Oracle	ORCL	FALSE
MySQL en Aceva D	X.XXX.XXX.XX	3306	MYSQL	Northwind	FALSE

Donde

Nombre de origen de datos
Identificador para distinguir de forma exclusiva la base de datos.

Dirección IP
Dirección IP del servidor o instancia de base de datos.

Puerto
Número de puerto para conectarse a la base de datos.

Tipo de base de datos
Tipo de base de datos como, por ejemplo, Oracle, MSSQL, Db2, Sybase, PostgreSQL o MySQL.

Nombre de base de datos
Nombre de la base de datos.

Suprimir
Toma como valor predeterminado FALSE para la creación del origen de datos. Si el valor se establece en TRUE, el origen de datos se suprime del servidor de IBM Data Risk Manager después de la operación de importación.

Con la información necesaria para cada base de datos de destino, se puede utilizar la plantilla de importación de definición de origen de datos de IBM Data Risk Manager para definir orígenes de datos.

Procedimiento

1. Defina información de origen de datos en el archivo de plantilla CSV.
2. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
3. Pulse el icono de menú de aplicación  .
4. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Descubrimiento nativo**.
5. Pulse **Importar**.
6. Para localizar y seleccionar el archivo CSV de definiciones de origen de datos, pulse **Seleccionar archivo**.
7. Pulse **Cargar**. Se mostrarán los orígenes de datos en la sección **Importar origen de datos**.

   Si se encuentra un error, tendrá que revisar el archivo CSV para corregir errores y volver a importar el archivo. Si la lista de orígenes de datos está estructurada de forma incorrecta o la lista de orígenes de datos contiene información incorrecta, la importación del archivo CSV podría fallar.
8. Especifique los parámetros de conexión con los orígenes de datos que se importan para establecer la conexión con la base de datos.
   a. Seleccione una base de datos y efectúe una doble pulsación.
   b. Establezca las opciones siguientes y pulse **Añadir**.

Adaptador	Nombre del recopilador de datos.
Agentes	Nombre de agente para conectarse a la base de datos.
Nombre de base de datos	Nombre de la base de datos.
Identificador	Nombre del origen de datos.

Nombre de usuario	Nombre del usuario de base de datos.
Contraseña	Contraseña para el nombre de usuario de base de datos.

9. Para ver los orígenes de datos que ha añadido, pulse **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**.

Inventario de aplicaciones

El inventario de aplicaciones de IBM Data Risk Manager está formado por aplicaciones, sus atributos y relaciones con otras entidades de negocio. Utilice el componente Gestionar inventario para ver y gestionar las aplicaciones que ha importado a través de archivos CSV como datos de contexto y sus asociaciones con otras entidades de negocio como, por ejemplo, orígenes de datos, infraestructuras alojadas y procesos de negocio.

IBM Data Risk Manager proporciona visibilidad de riesgos de activos de información en los datos de contexto empresarial de una organización. La visualización de riesgos de los activos de información requiere una captura e importación única inicial de los datos de contexto empresarial de la organización en lo que se refiere a unidades de negocio, líneas de negocio (LOB), procesos empresariales, aplicaciones y partes interesadas.

Importe los datos de contexto empresarial a IBM Data Risk Manager utilizando uno o varios archivos en el formato de valores separados por comas (CSV). A continuación, puede modificar y añadir datos de contexto de aplicación en función de sus necesidades.

Para obtener más información los datos de contexto empresarial, consulte "Correlación de datos de contexto empresarial" en la página 106.

Visualización de datos de inventario de aplicaciones

Puede ver e interactuar con datos de contexto de aplicación que están formados por aplicaciones, sus atributos y las relaciones con otras entidades.

Antes de empezar

Para ver y gestionar datos de inventario de aplicaciones, asegúrese de que los datos de contexto empresarial se han importado a IBM Data Risk Manager. Para obtener más información los datos de contexto empresarial, consulte "Correlación de datos de contexto empresarial" en la página 106.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Para ver la lista de aplicaciones, vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Aplicación**.

   Junto con el nombre de la aplicación, también puede ver información de origen de aplicación. Por ejemplo, `ServiceNow`, `OneTrust`, `Nativo` o `Registro`.

Origen de aplicación	Descripción
ServiceNow	Los datos se importan al inventario de IBM Data Risk Manager desde ServiceNow.
`OneTrust`	Los datos se importan al inventario de IBM Data Risk Manager desde OneTrust.
`Nativo`	Los datos se importan al inventario de IBM Data Risk Manager utilizando archivos CSV.

Origen de aplicación	Descripción
`Registro`	Los datos se añaden al inventario de aplicaciones de IBM Data Risk Manager utilizando el componente **Gestionar inventario**.

4. Seleccione una aplicación en la lista para ver sus propiedades bajo **Detalles de propiedad**.
5. Para añadir una aplicación al inventario, pulse el icono **Aplicación**  .
6. Para una aplicación seleccionada, puede ejecutar las operaciones siguientes.
   - Para modificar detalles de aplicación, pulse el icono **Editar**  .
   - Para suprimir una aplicación del inventario, pulse el icono **Suprimir**  .
   - Para asociar otras entidades de negocio con la aplicación, pulse el icono **Conectar**  .
7. Pulse **Renovar panel de control** para renovar el panel de control de IBM Data Risk Manager con los datos de contexto de aplicación modificados en los activos de información publicados.

Adición de una aplicación al inventario

Utilice el componente **Gestionar inventario** > **Aplicación** de IBM Data Risk Manager para añadir datos de contexto de aplicación al inventario.

Acerca de esta tarea

IBM Data Risk Manager proporciona visibilidad a los riesgos de activos de información en los datos de contexto empresarial de una organización en términos de aplicaciones, procesos de negocio, unidades de negocio, líneas de negocio (LOB) y partes interesadas. Puede importar datos de contexto de aplicación al inventario de IBM Data Risk Manager a través de archivos CSV. Para este inventario, puede añadir aplicaciones y sus propiedades de acuerdo con las necesidades de negocio. Para obtener más información los datos de contexto empresarial, consulte "Correlación de datos de contexto empresarial" en la página 106.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://`*`<dirección-IP-servidor-IDRM>`*`:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Aplicación**. Se muestra la lista de aplicaciones.
4. En la ventana **Aplicaciones**, pulse el icono **Aplicación**  .
5. En la ventana **Aplicación**, establezca las opciones siguientes.

Opción	Descripción
Nombre	Especifique un nombre para la aplicación que está añadiendo al inventario.
Nombre de visualización	Especifique el nombre de visualización de la aplicación.
Descripción	Añada una descripción para la aplicación que está añadiendo.

6. Para guardar los detalles de aplicación, pulse **Guardar**. La aplicación que ha añadido ahora se muestra en la lista de aplicaciones. Junto con el nombre de la aplicación, **Registro** indica que la aplicación se ha añadido al inventario utilizando el componente **Gestionar inventario**.
7. Defina las propiedades de aplicación.
   a) Seleccione la aplicación que ha añadido ahora desde la lista. Las propiedades de aplicación se muestran en la ventana **Detalles de propiedad**.

Estas propiedades se importan desde archivos CSV a IBM Data Risk Manager.

b) Especifique los valores apropiados a las propiedades.

c) Pulse **Guardar**.

Qué hacer a continuación

Conecte la aplicación que ha añadido ahora con otras entidades de negocio. Para obtener más información sobre la conexión, consulte "Asociación de aplicaciones con otras entidades de contexto empresarial " en la página 128.

Asociación de aplicaciones con otras entidades de contexto empresarial

Puede asociar las aplicaciones que ha añadido al inventario con las entidades de contexto empresarial apropiadas como, por ejemplo, orígenes de datos, infraestructuras alojadas o procesos de negocio basados en los requisitos. También puede modificar los detalles de conexión de las aplicaciones existentes que ha importado utilizando archivos CSV.

Acerca de esta tarea

Para obtener más información los datos de contexto empresarial, consulte "Correlación de datos de contexto empresarial" en la página 106.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Aplicación**. Se muestra la lista de aplicaciones.
4. Desde la lista, seleccione una aplicación que desea asociar a otras entidades de negocio.
5. Pulse el icono **Conectar**  .
6. Conecte la aplicación con otras entidades de negocio basándose en sus necesidades empresariales.

   Procesos de negocio

   a. Pulse **Correlación de procesos de negocio**.

   b. Desde la lista **Todos los procesos de negocio**, seleccione los procesos de negocio para asociar a la aplicación.

   c. Pulse el icono de flecha de avance  .

   Orígenes de datos

   a. Pulse **Correlación de orígenes de datos**.

   b. Desde la lista **Todos los orígenes de datos**, seleccione los orígenes de datos para asociar a la aplicación.

   c. Pulse el icono de flecha de avance  .

   Infraestructuras

   a. Pulse **Correlación de servidores alojados**.

   b. Desde la lista **Todos los servidores alojados**, seleccione los servidores para asociar a la aplicación.

   c. Pulse el icono de flecha de avance  .
7. Si desea cancelar alguna de las selecciones, ejecute los pasos siguientes.

a) Elija los elementos que desee cancelar desde la lista seleccionada de procesos de negocio, orígenes de datos o servidores alojados.

b) Pulse el icono de flecha hacia atrás .

8. Pulse **Guardar conexión** para guardar los detalles de conexión.

Inventario de procesos de negocio

El inventario de procesos de negocio de IBM Data Risk Manager está formado por procesos empresariales, sus atributos y las relaciones con otras entidades de negocio. Utilice el componente Gestionar inventario para ver y gestionar los procesos de negocio que ha importado a través de archivos CSV como datos de contexto y sus asociaciones con otra entidad de negocio como, por ejemplo, aplicaciones.

IBM Data Risk Manager proporciona visibilidad de riesgos de activos de información en los datos de contexto empresarial de una organización. La visualización de riesgos de los activos de información requiere una captura e importación única inicial de los datos de contexto empresarial de la organización en lo que se refiere a unidades de negocio, líneas de negocio (LOB), procesos empresariales, aplicaciones y partes interesadas.

Importe los datos de contexto empresarial a IBM Data Risk Manager utilizando uno o varios archivos en el formato de valores separados por comas (CSV). A continuación, puede modificar y añadir datos de contexto del proceso de negocio en función de sus necesidades.

Para obtener más información los datos de contexto empresarial, consulte "Correlación de datos de contexto empresarial" en la página 106.

Visualización de datos de inventario del proceso de negocio

Puede ver e interactuar con datos de inventario del proceso de negocio que están formados por procesos de negocio, sus atributos y las relaciones con otras entidades.

Antes de empezar

Para ver y gestionar datos de inventario de proceso de negocio, asegúrese de que los datos de contexto empresarial se han importado a IBM Data Risk Manager. Para obtener más información los datos de contexto empresarial, consulte "Correlación de datos de contexto empresarial" en la página 106.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Para ver la lista de procesos de negocio, vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Proceso de negocio**.

   Junto con el nombre del proceso de negocio, también puede ver información de origen. Por ejemplo, `Nativo` o `Registro`.

Origen de proceso de negocio	Descripción
`Nativo`	El proceso de negocio se importa al inventario de IBM Data Risk Manager utilizando archivos CSV.
`Registro`	El proceso de negocio se añade al inventario de IBM Data Risk Manager utilizando el componente **Gestionar inventario**.

4. Seleccione un proceso de negocio en la lista para ver sus propiedades bajo **Detalles de propiedad**.
5. Para añadir un proceso de negocio al inventario, pulse el icono **Proceso de negocio** .

6. Para un proceso de negocio seleccionado, puede ejecutar las operaciones siguientes.
   - Para modificar detalles del proceso de negocio, pulse el icono **Editar** .
   - Para suprimir un proceso de negocio del inventario, pulse el icono **Suprimir** .
   - Para asociar otras entidades de negocio con el proceso, pulse el icono **Conectar** .
7. Pulse **Renovar panel de control** para renovar el panel de control de IBM Data Risk Manager con los datos de contexto del proceso de negocio modificados en los activos de información publicados.

Adición de un proceso de negocio al inventario

Utilice el componente **Gestionar inventario** > **Proceso de negocio** de IBM Data Risk Manager para añadir datos de contexto de proceso de negocio al inventario.

Acerca de esta tarea

IBM Data Risk Manager proporciona visibilidad a los riesgos de activos de información en los datos de contexto empresarial de una organización en términos de aplicaciones, procesos de negocio, unidades de negocio, líneas de negocio (LOB) y partes interesadas. Puede importar datos de contexto de proceso de negocio al inventario de IBM Data Risk Manager a través de archivos CSV. Para este inventario, puede añadir procesos de negocio y sus propiedades de acuerdo con sus necesidades de negocio. Para obtener más información los datos de contexto empresarial, consulte "Correlación de datos de contexto empresarial" en la página 106.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Proceso de negocio**. Se muestra la lista de procesos de negocios.
4. En la ventana **Procesos de negocio**, pulse el icono **Proceso de negocio** .
5. En la ventana **Proceso de negocio**, establezca las opciones siguientes:

Opción	Descripción
Nombre	Especifique un nombre para el proceso de negocio que está añadiendo al inventario.
Nombre de visualización	Especifique el nombre de visualización del proceso de negocio.
Descripción	Añada una descripción para el proceso de negocio que está añadiendo.

6. Para guardar los detalles del proceso de negocio, pulse **Guardar**. Los procesos que ha añadido ahora se muestran en la lista de procesos de negocio. Junto con el nombre del proceso de negocio, **Registro** indica que el proceso se ha añadido al inventario utilizando el componente **Gestionar inventario**.
7. Defina las propiedades de proceso de negocio.
   a) Seleccione el proceso de negocio que ha añadido ahora desde la lista. Las propiedades del proceso de negocio se visualizan en la ventana **Detalles de propiedad**.

      Estas propiedades se importan desde archivos CSV a IBM Data Risk Manager.
   b) Especifique los valores apropiados a las propiedades.
   c) Pulse **Guardar**.

Qué hacer a continuación
Conecte el proceso de negocio que ha añadido ahora con otras entidades de negocio. Para obtener más información sobre la conexión, consulte "Asociación de un proceso de negocio con otras entidades de negocio " en la página 131.

Asociación de un proceso de negocio con otras entidades de negocio
Puede asociar los procesos de negocio que ha añadido al inventario con la entidad de contexto empresarial apropiada como, por ejemplo, aplicaciones basadas en los requisitos. También puede modificar los detalles de conexión de los procesos de negocio existentes que ha importado utilizando archivos CSV.

Acerca de esta tarea
Para obtener más información los datos de contexto empresarial, consulte "Correlación de datos de contexto empresarial" en la página 106.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Proceso de negocio**. Se muestra la lista de procesos de negocios.
4. Desde la lista, seleccione un proceso de negocio que desee asociar a otra entidad de negocio como, por ejemplo, una aplicación.
5. Pulse el icono **Conectar**  .
6. Conecte el proceso de negocio con las aplicaciones.
   a. Pulse **Correlación de aplicaciones**.
   b. Desde la lista **Todas las aplicaciones**, seleccione aplicaciones para asociar al proceso de negocio.
   c. Pulse el icono de flecha de avance  .
7. Si desea cancelar alguna de las selecciones, ejecute los pasos siguientes.
   a) Seleccione las aplicaciones en la lista **Aplicaciones seleccionadas**.
   b) Pulse el icono de flecha hacia atrás  .
8. Pulse **Guardar conexión**.

Inventario de amenazas

El inventario de amenazas de IBM Data Risk Manager está constituido de posibles amenazas sobre la los activos de información y sus propiedades. Utilice el componente Gestionar inventario para ver y gestionar la información de amenazas.

Vaya a **IBM Data Risk Manager** > **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Amenaza** para ver y gestionar amenazas.

Visualización de datos de inventario de amenazas

Puede ver e interactuar fácilmente con los datos de inventario de amenazas que están formados por amenazas, sus propiedades y los planes de acción.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).

2. Pulse el icono de menú de aplicación .
3. Para ver la lista de amenazas, vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Amenaza**.
4. Para añadir una amenaza al inventario, pulse el icono **Añadir** .
5. Para modificar detalles de amenaza, seleccione una amenaza en la lista y pulse el icono **Editar** .
6. Para renovar la lista de inventario de amenazas, pulse el icono **Renovar** .

Adición de una amenaza al inventario

Puede definir posibles amenazas y sus propiedades en IBM Data Risk Manager para el análisis de riesgos y acciones.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Amenaza**.
4. En la página **Amenaza**, pulse el icono **Añadir** .
5. En la ventana **Amenaza**, establezca las opciones siguientes.

Opción	Descripción
Nombre de amenaza	Especifique un nombre para la amenaza que está añadiendo al inventario.
Tipo de amenaza	Seleccione el tipo de amenaza.
Categoría	Especifique la categoría de amenaza.
Descripción de la amenaza	Añada más información sobre la amenaza que está añadiendo.
Ponderación relativa	Asigne una ponderación relativa a la amenaza.
Impacto	Especifique el posible impacto de la amenaza.
Probabilidad	Especifique la probabilidad de que se produzca la amenaza.
Activo	El botón de conmutador habilitado indica que la amenaza está en un estado activo.
Syslog	Habilite el botón de conmutador para especificar detalles para crear la amenaza basándose en las alertas del syslog. a. Pulse **Siguiente**. b. Especifique detalles en los campos siguientes. • **Número de días** • **Duración** • **Rango de umbrales** • **Dirección IP** • **Día de la semana específico** • **Gravedad** • **Políticas**

6. Pulse **Siguiente**.
7. Seleccione las actividades de reparación apropiadas y las tareas.
8. Pulse **Guardar**.

Paquetes de soluciones

IBM Data Risk Manager permite la definición y el desarrollo de políticas y reglas específicas para cubrir los requisitos de los clientes relacionados con el descubrimiento y la clasificación y la integración de controles. Se proporciona un conjunto de políticas y reglas predefinidas para cubrir los requisitos comunes de los clientes, tales como el descubrimiento de información identificable personalmente (PII). Los paquetes de soluciones para políticas y reglas y sus atributos se pueden personalizar en función del contexto de la organización, por ejemplo, la plataforma de base de datos, los tipos y los convenios de nombres.

Durante la fase inicial de un proyecto, los requisitos de las políticas y reglas se capturan mediante entrevistas y talleres con las partes interesadas empresariales y técnicas importantes. En función de los requisitos específicos del cliente, se pueden personalizar y preparar los paquetes de soluciones en el formato necesario. A continuación, se pueden importar los paquetes de soluciones a IBM Data Risk Manager.

Importar paquetes de soluciones

Utilice el componente Modelador de contexto empresarial de IBM Data Risk Manager para importar paquetes de soluciones. El paquete de soluciones contiene un conjunto de políticas y reglas predefinidas para cubrir los requisitos comunes de los clientes, tales como el descubrimiento de información identificable personalmente (PII).

Antes de empezar

Asegúrese de que los paquetes de soluciones estén disponibles para importarlos.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Paquete de solución**.
4. Pulse **Seleccionar archivo** para cargar los archivos de **Paquete de solución**, **Políticas** y **Tareas**.
   Pulse los botones respectivos para ver el contenido en la sección de vista previa.
5. Pulse **Importar** para importar los paquetes de soluciones.

Qué hacer a continuación

Para verificar que se han importado correctamente los paquetes de soluciones, vaya a **Modelador de contexto empresarial** > **Central de gestión de políticas**.

Gestión de programas

El programa IBM Data Risk Manager representa un esfuerzo de descubrimiento, clasificación e integración de controles definidos para una o más áreas o líneas de negocio, grupos de organizaciones, aplicaciones, procesos empresariales y otras entidades específicas de la organización.

IBM Data Risk Manager permite a las organizaciones enfocar la seguridad de datos de forma específica definiendo mediante programación objetivos y el ámbito para una iniciativa de descubrimiento y clasificación de datos. A menudo, las organizaciones se embarcan en el descubrimiento y la clasificación de datos a gran escala que contiene muchas áreas, aplicaciones y procesos empresariales. En IBM Data Risk Manager, puede ver orígenes de datos, estructurados y no estructurados, por entidades diferentes, como áreas de negocio, líneas de negocio, aplicaciones y procesos empresariales. Solo se pueden incluir fuentes de datos relevantes para el compromiso de descubrimiento y clasificación, dando prioridad a la más valiosa o a la más susceptible de contener datos críticos de la organización.

El ámbito es una actividad que establece o correlaciona los límites de la evaluación de riesgos que se va a realizar. El ámbito se debe llevar a cabo en una fase temprana del proyecto basándose en la información que se captura mediante entrevistas y talleres con los patrocinadores y los principales interesados.

Creación de un programa

Utilice IBM Data Risk Manager para crear un programa que defina y cree un ámbito de información empresarial basándose en áreas de negocio, líneas de negocio, aplicaciones, procesos y otros metadatos de contexto empresarial de la organización.

Acerca de esta tarea

Tenga en cuenta los factores siguientes para crear programas y subprogramas.

- Se puede crear cualquier número de subprogramas o programas hijo para un programa padre.
- Puede crear un programa como padre o como programa hijo. De forma predeterminada, el programa se crea como programa padre. Cuando se selecciona la opción de subprograma, debe proporcionar detalles del programa padre y guardar el subprograma.
- Cuando se visualizan detalles de un programa en la página Cartera de programas, también se visualiza la información de subprogramas.
- Cuando se selecciona un programa padre, se enumeran también todos sus subprogramas, si se han creado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Inicio**.
4. En la página **Cartera de programas**, pulse el icono **Añadir programa**  para crear un programa.
5. Establezca las opciones siguientes y pulse **Guardar**.

Opción	Descripción
Nombre	Especifique un nombre para el programa.
Propietario	Seleccione un propietario de programa de la lista de usuarios. Para visualizar la lista, pulse el icono  .
Descripción	Especifique la información adicional que indica la finalidad del programa que está creando.
Fecha de inicio	Especifique la fecha de inicio del programa.
Fecha de finalización	Especifique la fecha de finalización del programa.

6. Cuando se guarda el programa, se visualiza el mensaje siguiente. Pulse **Sí** para asignar un usuario, un grupo de usuarios y el ámbito del programa.

```
El programa se ha guardado correctamente. ¿Desea crear el ámbito de titularidades para el
programa?
```

7. Asigne usuarios, grupos de usuarios y el ámbito del programa. A continuación, pulse **Asignar**.
   a) Para asignar usuarios, seleccione los usuarios en **Usuarios**. Los usuarios asignados pueden acceder a los datos que se descubren de acuerdo con el ámbito del programa.
   b) Para asignar grupos de usuarios, seleccione los grupos en **Grupo de usuarios**.
   c) Para crear el ámbito del programa, seleccione las entidades de contexto empresarial necesarias bajo **Ámbito**. Las entidades de contexto empresarial se importan de varios orígenes.

      Puede asignar las entidades de contexto empresarial siguientes.

      - Línea de negocio (LOB)
      - Aplicación
      - Plataforma
      - Conformidad
      - Entorno
      - Recurso
      - Origen de datos

      Nota: Si las entidades de contexto empresarial no están seleccionadas, el ámbito del programa incluye todos los orígenes de datos disponibles. El ámbito de programa se establece en todo incluido de forma predeterminada.
8. Pulse **Evidencia** para crear y asociar una evidencia con el programa.

Gestión de políticas

Una política es un conjunto de operaciones que desea que realice IBM Data Risk Manager. Utilice IBM Data Risk Manager para definir las políticas y reglas asociadas para el descubrimiento y la clasificación de datos, la limpieza y el análisis, y los controles como, por ejemplo, la supervisión de actividad de base de datos.

Utilice **Suite de aplicaciones de IBM Data Risk Manager** > **Modelador de contexto empresarial** > **Central de gestión de políticas** para definir y desplegar las políticas de IBM Data Risk Manager. IBM Data Risk Manager contiene los tipos de políticas siguientes.

- Políticas creadas en IBM Data Risk Manager.
- Políticas y reglas importadas a través de paquetes de solución.

Puede gestionar las políticas siguientes en IBM Data Risk Manager.

Descubrimiento y clasificación de datos
Políticas de clasificación de IBM Security Guardium para el descubrimiento de datos.

Política de entorno de trabajo de análisis
Reglas de análisis nativo de IBM Data Risk Manager para la agrupación de activos de información.

Supervisión de actividad de base de datos (DAM)
Políticas de supervisión de actividad de base de datos de IBM Security Guardium para las violaciones de política de seguridad.

Puede desplegar políticas y reglas en una aplicación utilizando Suite de aplicaciones de IBM Data Risk Manager. Por ejemplo, puede definir las políticas de DAM de IBM Security Guardium en la Central de gestión de políticas y, a continuación, desplegarlas en sistemas de IBM Security Guardium como Gestor central, Recopilador o Agregador en función de su disponibilidad en el servidor de IBM Data Risk Manager.

Creación de una política de entorno de trabajo de análisis para orígenes de datos

Puede crear políticas de entorno de trabajo de análisis en IBM Data Risk Manager para definir reglas personalizadas para la creación de grupos de activos de información al completar exploraciones de metadatos en orígenes de datos estructurados de destino. Las políticas que se importan como parte de los paquetes de solución están disponibles en el entorno de trabajo de análisis para crear grupos de activos de información.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú .
3. Vaya a **Modelador de contexto empresarial** > **Central de gestión de políticas**.
4. Pulse el icono **Seleccionar tipo de política** y seleccione **Política de entorno de trabajo de análisis**.
5. Pulse **Estructurados**.
6. Para crear una política de entorno de trabajo de análisis para orígenes de datos estructurados, pulse el icono **Añadir nueva política** en la sección **Detalles**.
7. En **Creador de limpieza de políticas**, establezca las opciones siguientes para crear una nueva política.

Opción	Descripción
Nombre	Especifique el nombre de la política de análisis.
Descripción	Añada una descripción para la política de análisis.
Nombre de conjunto de reglas	Especifique el nombre del conjunto de reglas.
Categoría	Seleccione la categoría de política de análisis en la lista.
Clasificación	Seleccione en la lista la clasificación de política.
Activo	Especifique el nombre de activo.

8. Pulse el icono **Añadir regla** para añadir una regla de `limpieza`.

   Las reglas del entorno de trabajo de análisis se pueden utilizar para definir patrones de metadatos para ejecutar las coincidencias de datos en los nombres de tabla y los nombres de columna.

Opción	Descripción
Descripción de regla nueva	Especifique el nombre de la regla.
Operaciones	Seleccione el tipo de operación de la lista que especifica las condiciones para llevar a cabo una coincidencia para la regla.
Aplicado en	Incluir detalles de tabla para una coincidencia.
Patrón	Especifique una coincidencia exacta para un patrón de descubrimiento de una regla de análisis nativo.
Sinónimos	Especifique varios patrones de descubrimiento para una regla de análisis nativo.

9. Cree una regla adicional para identificar los nombres de tabla y columna que contienen un patrón o sinónimo específico.

10. Pulse **Guardar** para guardar los detalles de la política y de la regla.

    La política de análisis se puede utilizar para la agrupación de activos de información para las exploraciones de metadatos que se realizan en IBM Data Risk Manager.

Creación de una política de entorno de trabajo de análisis para orígenes de datos no estructurados

Puede crear políticas de entorno de trabajo de análisis en IBM Data Risk Manager para identificar los falsos positivos y clasificar los metadatos no estructurados en los orígenes de datos no estructurados de destino.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú .
3. Vaya a **Modelador de contexto empresarial** > **Central de gestión de políticas**.
4. Pulse el icono **Seleccionar tipo de política** y seleccione **Política de entorno de trabajo de análisis**.
5. Pulse **Sin estructurar**.
6. Para crear una política de entorno de trabajo de análisis para orígenes de datos no estructurados, pulse el icono **Añadir nueva política** en la sección **Detalles**.
7. En **Creador de políticas no estructuradas**, establezca las opciones siguientes para crear una nueva política.

Opción	Descripción
Nombre	Especifique el nombre de la política de análisis.
Descripción	Añada una descripción para la política de análisis.
Etiqueta de política	Especifique el nombre de etiqueta de política
Nombre de activo	Especifique el nombre de activo.

8. Pulse el icono **Añadir regla** para añadir una regla.
9. Seleccione un tipo de regla bajo **Basado en contenido** o **Propiedades de archivo** según los requisitos.
10. Pulse **Siguiente**.
11. Especifique un nombre para la regla.
12. Especifique el nombre de activo.
13. Especifique los demás criterios de regla para el tipo de regla seleccionado según los requisitos.
14. Seleccione una regla adicional en **Basado en contenido** o **Propiedades de archivo**, según sus requisitos.
15. Pulse **Guardar** para guardar los detalles de la política y de la regla.

    La política de análisis se puede utilizar para la agrupación de activos de información para las exploraciones de metadatos que se ejecutan en IBM Data Risk Manager en los orígenes de datos no estructurados.

Modificación de una política

Las políticas definidas en la Central de gestión de políticas de IBM Data Risk Manager se pueden editar con el fin de añadir y actualizar reglas, parámetros y valores para cumplir los requisitos.

Acerca de esta tarea

Nota: Las políticas importadas de IBM Security Guardium y que ya están desplegadas en IBM Security Guardium no se pueden editar.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú .
3. Vaya a **Modelador de contexto empresarial** > **Central de gestión de políticas**.
4. Pulse el icono **Seleccionar tipo de política** para seleccionar un tipo de política para mostrar las políticas.
5. Seleccione una política que desee editar de la lista de políticas.
6. Pulse el icono **Editar** .
7. En la página del creador de políticas, modifique los detalles de política de acuerdo con sus requisitos.

   Para añadir una regla para la política:

   a. Pulse el icono **Añadir regla** .
   b. Especifique la definición de regla de acuerdo con sus requisitos.

   Para editar una información de regla para la política:

   a. Seleccione una regla de la lista para editarla.
   b. Pulse el icono Editar y realice los cambios necesarios.

   Para eliminar una regla para la política

   a. Seleccione una regla de la lista para suprimirla.
   b. Pulse el icono Suprimir .
8. Pulse **Guardar** para guardar los cambios.

Clonación de políticas

Utilice la función clonar de IBM Data Risk Manager para crear una copia de una política existente con un nombre nuevo.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú .
3. Vaya a **Modelador de contexto empresarial** > **Central de gestión de políticas**.
4. Pulse el icono **Seleccionar tipo de política** para seleccionar un tipo de política para visualizar las políticas.
5. Seleccione una política que desee clonar de la lista de políticas.
6. Pulse el icono **Clonar** .
7. Pulse **Sí** en el diálogo de confirmación.
8. Especifique un nuevo nombre para la política.
9. Pulse **Aceptar** para clonar la política existente.

Eliminación de una política

Puede suprimir políticas de IBM Data Risk Manager si ya no son necesarias.

Acerca de esta tarea

Nota: Las políticas importadas de IBM Security Guardium y que ya están desplegadas en IBM Security Guardium no se pueden suprimir.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador.
2. Pulse el icono de menú .
3. Vaya a **Modelador de contexto empresarial** > **Central de gestión de políticas**.
4. Pulse el icono **Seleccionar tipo de política** para seleccionar un tipo de política para visualizar las políticas.
5. Seleccione una política que desee eliminar de la lista de políticas.
6. Pulse el icono **Suprimir** .
7. Pulse **Sí** para eliminar la política.

Panel de control del Centro de control y mandatos de seguridad

El panel de control del Centro de control y mandatos de seguridad (SC3), la página de destino del componente SC3 de IBM Data Risk Manager, muestra una representación gráfica de los orígenes de datos, los activos de información, el estado de los procesos de exploración de seguridad y los detalles de transacción asociados con el programa y el usuario especificado. La representación gráfica de los datos le ayuda a comprender e interpretar fácilmente la información.

El componente SC3 de IBM Data Risk Manager se utiliza para ejecutar las exploraciones de descubrimientos de datos en los orígenes de datos definidos. Los resultados de datos descubiertos se utilizan entonces para analizar, filtrar y categorizar los activos de información.

El panel de control de SC3 contiene los widgets siguientes.

- Procesos de exploración de seguridad y estado
- Visualizador de datos
- Activos de información/orígenes de datos

Puede personalizar colores predeterminados de los elementos de widgets con los colores configurados por el usuario de acuerdo con sus requisitos. Para ver los pasos sobre cómo personalizar los colores, consulte “Configuración de esquemas de color para visualizaciones de widgets” en la página 172.

Acceso al panel de control de SC3

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) con sus credenciales de usuario.
2. Pulse el icono de menú .
3. Vaya a **Centro de control y mandatos de seguridad** > **Programa**.
4. Seleccione un programa para el que desee ver el origen de datos y la información de exploración y ejecutar operaciones de descubrimiento y clasificación.

   Se muestra la página del panel de control **Centro de control y mandatos de seguridad** > **Inicio**.

Procesos de exploración de seguridad y estado

El widget Procesos de exploración de seguridad y estado proporciona una vista consolidada de los procesos de exploración de seguridad y su estado. Puede ver la información siguiente.

- Una lista de los procesos de clasificador de datos ejecutados durante el último mes, junto con su estado, en **Exploraciones recientes**. La lista muestra los procesos activados y de descarga de datos estructurados y no estructurados. Pulse el icono ••• en un proceso de exploración para ver los detalles de los orígenes de datos asociados.
- Una lista de los procesos de evaluación de vulnerabilidades, y su estado, para los procesos activados y descargados en **Procesos de evaluación de vulnerabilidades**. Pulse el icono ••• en un proceso de exploración para ver los detalles de los orígenes de datos asociados.
- Muestra el porcentaje acumulativo de orígenes de datos explorados durante los últimos 6 meses. Se muestra el porcentaje para los estados, como por ejemplo **Completado**, **Erróneo**, **Planificado**, **En curso**, **En cola** y **Nuevo**.
- Un gráfico de barras que muestra los recuentos de tablas numéricas de los orígenes de datos explorados durante los últimos 6 meses. En el gráfico, el eje X representa la línea temporal (mes o día). Si las exploraciones se ejecutan durante menos de 60 días, el tiempo se representa en días. Si las exploraciones se ejecutan durante más de 60 días, el tiempo se representa en meses. El eje Y representa el recuento de tablas de base de datos (datos estructurados de exploraciones descargadas y activadas) y los archivos (datos no estructurados). Pase el cursor sobre una barra para ver los recuentos de tablas para una línea temporal específica. Solo se muestra el recuento individual de las tablas en las categorías de datos **Sin limpiar** y **Etiquetado** de la página **Entorno de trabajo de análisis**. El recuento no incluye el número de tablas en las categorías de datos **Excluido** y **Exportado**. Puede ver los datos según **Tipos de transacción**, **Origen** y **Plataforma**. Pulse la barra para ver la información asociada en **Detalles de transacción**.

Visualizador de datos

El visualizador de datos es una representación visual de los orígenes de datos que están en el ámbito, que se sobrescribe con la información de metadatos empresariales. De forma predeterminada, el visualizador representa todos los orígenes de datos según la Línea de negocio (LOB). Al pulsar en el icono **LOB**, se muestra el recuadro de lista **Seleccionar elementos para gráfico** si los elementos son más de 10. El diagrama de visualización se muestra en el widget Visualizador de datos para los atributos seleccionados. Para ver información más detallada, ejecute los pasos siguientes.

1. En el widget Visualizador de datos, pulse el icono **Expandir** .
2. En la vista Visualizador de datos expandida, pulse el icono de atributos del diagrama.

Ejecute los pasos siguientes para configurar el visualizador.

1. En la vista Visualizador de datos expandida, pulse el icono Valores del visualizador .
2. Realice la selección necesaria de los atributos en la lista.

En la vista Visualizador de datos expandida, pulse el icono **Contraer** para visualizar la página del panel de control de SC3.

Activos de información/orígenes de datos

Activos de información
Muestra recuentos de activos de información para el programa seleccionado en el gráfico de anillo y en la vista de lista para los estados como por ejemplo **Publicado** y **En revisión**.

Orígenes de datos
Muestra los recuentos de orígenes de datos para el programa seleccionado en un gráfico de anillo, y también en la vista de lista según los resultados de la exploración de descubrimiento de datos, como por ejemplo **Descubiertos**, **Erróneos**, **Por descubrir** y **Planificados**.

Descubrimiento de datos

Utilice el componente Centro de control y mandatos de seguridad (SC3) de IBM Data Risk Manager para ejecutar las exploraciones de descubrimientos de datos en los orígenes de datos definidos. Los resultados de datos descubiertos se utilizan entonces para analizar, filtrar y categorizar los activos de información.

El Asistente de ingesta de datos (DIW) se puede utilizar para ejecutar los procesos de descubrimiento en función de políticas y criterios definidos mediante la planificación de trabajos a través de exploraciones de IBM Security Guardium o exploraciones de descubrimientos de metadatos nativos. Puede importar también las exploraciones de clasificador de IBM Security Guardium en IBM Data Risk Manager para el análisis de datos .La definición de taxonomía y la clasificación de los elementos de datos descubiertos se realizan basándose en el análisis de metadatos para la información descubierta y los activos de datos.

Ejecución de la exploración de descubrimiento de datos utilizando IBM Security Guardium

Utilice el componente Centro de control y mandatos de seguridad (SC3) de IBM Data Risk Manager para ejecutar la exploración de clasificador de IBM Security Guardium.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security Guardium. Para obtener información sobre la integración, consulte “Integración de IBM Security Guardium con IBM Data Risk Manager” en la página 38.

Asegúrese de que se importan los datos de contexto empresarial necesarios y que dispone de un programa con el ámbito adecuado para ejecutar la operación de descubrimiento de datos.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`) con privilegios de administrador.
2. Pulse el icono de menú .
3. Vaya a **Centro de control y mandatos de seguridad** > **Programa**.
4. Seleccione un programa en el que desea realizar el descubrimiento y la clasificación.

   El visualizador de datos se muestra en la página **Centro de control y mandatos de seguridad - Panel de control**.

   El visualizador de datos es una representación visual de los orígenes de datos que están en el ámbito que se sobrescribe con la información de metadatos empresariales. Puede configurar la descomposición del árbol de visualización ejecutando los pasos siguientes.

   a. Pulse el icono de menú .
   b. Seleccione los atributos de la lista desplegable de acuerdo con sus requisitos.
   c. Pulse **Hecho**.

   En función de la configuración, puede ver la información detallada efectuando una pulsación en cada nodo del árbol.
5. Vaya a **Centro de control y mandatos de seguridad** > **Inventario**.
6. Pulse el icono **Cambiar recopilador** .
7. Seleccione **IBM Guardium**.
8. Seleccione los orígenes de datos de la lista **Inventario de orígenes de datos**.

9. Seleccione las políticas de la lista **Inventario de políticas**.
10. Pulse el icono **Activar asistente de exploración**  .
11. Especifique un nombre para el proceso de clasificación.
12. Según sus requisitos, seleccione los recuadros de selección para incluir **Tablas de usuario**, **Vista** o **Tablas del sistema** en la exploración.

Ejecución de exploraciones de metadatos nativos

Utilice el componente Centro de control y mandatos de seguridad (SC3) de IBM Data Risk Manager para ejecutar la exploración de metadatos nativos de IBM Data Risk Manager en orígenes de datos estructurados y no estructurados.

Antes de empezar

Asegúrese de que se importan los datos de contexto empresarial necesarios y que dispone de un programa con el ámbito adecuado para ejecutar la exploración de descubrimiento de datos.

Para ejecutar una exploración de metadatos en bases de datos Oracle, el usuario debe tener el permiso para acceder a los objetos de la base de datos (dba_objects). Ejecute el mandato siguiente para proporcionar acceso al usuario.

```
otorgar sesión de creación, seleccione cualquier diccionario en <nombre_usuario>;
```

Acerca de esta tarea

Se da soporte a los documentos siguientes para la exploración no estructurada.

- HTML (HyperText Markup Language)
- XML (Extensible Markup Language)
- Formatos de documento de Microsoft Office
- PDF (Portable Document Format)
- RTF (Rich Text Format)
- Formatos de compresión y empaquetado
- Formatos de texto
- Archivos de clases Java
- Código fuente
- Archivos de registro
- Archivos de valores separados por comas (CSV)

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`) con privilegios de administrador.
2. Pulse el icono de menú  .
3. Vaya a **Centro de control y mandatos de seguridad** > **Programa**.
4. Seleccione un programa en el que desea realizar el descubrimiento y la clasificación.

   Se muestra el panel de control del Centro de control y mandatos de seguridad (SC3). El panel de control muestra una representación gráfica de los orígenes de datos, activos de información, estado de procesos de exploración de seguridad y detalles de transacción asociados con el programa seleccionado.
5. Pulse **Inventario**.
6. Pulse el icono **Cambiar recopilador**  .

7. Para ejecutar la exploración en orígenes de datos estructurados, seleccione **Nativo con estructura**.
8. Para ejecutar la exploración en orígenes de datos no estructurados, seleccione **Nativo sin estructura**.
9. Seleccione los orígenes de datos de la lista **Inventario de orígenes de datos**.
10. Seleccione las políticas de la lista **Inventario de políticas**.

    Nota: No hay políticas para la metaexploración estructurada.

11. Pulse el icono **Activar asistente de exploración**  .
12. Especifique un nombre para el proceso de clasificación en **Escribir nombre de proceso de clasificación**.
13. Para orígenes de datos estructurados, especifique los detalles siguientes.
    a. Según sus requisitos, seleccione los recuadros de selección para incluir **Tablas de usuario**, **Vista** o **Tablas del sistema** en la exploración.
    b. Seleccione **Habilitar recuento de filas** para visualizar el número de filas en las tablas de orígenes de datos.
14. Para iniciar inmediatamente la exploración, seleccione **Explorar ahora**.
15. Para iniciar la exploración más tarde, seleccione **Explorar después** y especifique las planificaciones.
16. Para iniciar el proceso, pulse **Activar exploración de metadatos**.
17. Para ver el estado de la exploración, vaya a **Centro de control y mandatos de seguridad** > **Inicio**.

Visualización de resultados de exploración de descubrimiento de datos

Utilice el componente Centro de control y mandatos de seguridad (SC3) de IBM Data Risk Manager para ver los resultados de exploración de descubrimiento de datos para realizar un análisis y acciones adicionales.

Antes de empezar

Puede ver las exploraciones completadas junto con el estado. Para ver el estado, vaya a **Centro de control y mandatos de seguridad** > **Inicio**.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`) con privilegios de administrador.
2. Pulse el icono de menú  .
3. Seleccione un programa de la lista.
4. Vaya a **Centro de control y mandatos de seguridad** > **Análisis**.
5. En **Lista de bases de datos**, seleccione el origen de datos para el que necesita revisar los resultados de exploración.
6. En la página **Entorno de trabajo de análisis**, se muestran las tablas y columnas para la base de datos de destino identificada y las coincidencias adecuadas si se ha aplicado una política durante la exploración de clasificación.
7. Asegúrese de que se completan las exploraciones para todos los orígenes de datos, que están en el ámbito respecto de las políticas que coinciden con el contenido de los orígenes de datos.

Importación de exploraciones de clasificador desde IBM Security Guardium

Puede importar las exploraciones de clasificador de dispositivos de IBM Security Guardium al inventario de IBM Data Risk Manager para clasificar datos y analizar riesgos.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security Guardium. Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium con IBM Data Risk Manager" en la página 38.

Acerca de esta tarea

El icono de transacción  indica que la operación de importación anterior se ha realizado correctamente.

El icono de transacción  indica que la operación de importación anterior ha fallado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Exploraciones de datos**.
4. Importe las exploraciones de datos.
   a) Pulse el icono **Descargar**  .
   b) En la ventana **Importar**, seleccione **Clasificador**.
   c) Desde la lista **Adaptador**, seleccione **IBM Guardium**.
   d) En la lista **Instancias**, seleccione una instancia de adaptador. Puede seleccionar hasta tres instancias.
   e) Seleccione la fecha a partir de la que desea extraer las exploraciones de IBM Security Guardium.
   f) Para importar todos los procesos que están asociados a las instancias seleccionadas, pulse **Importar**.
   g) Para importar solo los procesos de IBM StoredIQ que necesita de las instancias seleccionadas, ejecute los pasos siguientes.
      1) Pulse **Importar con selección de procesos**.
      2) Seleccione los procesos que necesaria importar de cada instancia de adaptador.
      3) Pulse **Importar**.
5. En la página **Exploraciones de datos**, puede ver las exploraciones que ha importado ahora.
6. Para renovar la lista de inventario de exploraciones de datos, pulse el icono **Renovar**  .
7. De forma alternativa, para ver los resultados de exploración después de la operación de importación, vaya a **Centro de control y mandatos de seguridad** > **Inicio**.

Limpieza y análisis de datos

Utilice el componente Centro de control y mandatos de seguridad (SC3) de IBM Data Risk Manager para la limpieza y el análisis de los resultados de exploración de descubrimientos de datos.

La función de limpieza y análisis de IBM Data Risk Manager incluye las tareas siguientes.

- Visualización de los resultados del descubrimiento.
- Aplicación de las reglas de filtrado.
- Exportación de los resultados a la taxonomía.

Durante el análisis de los resultados de exploración de descubrimientos de datos, los datos se agrupan en las categorías siguientes.

Sin limpiar
Lista el esquema, las tablas y las columnas que no se analizan (resultados de exploración de descubrimientos de datos).

Etiquetado
Lista las tablas y las columnas que son el resultado de aplicar una o varias políticas y reglas de filtrado.

Excluido
Lista las tablas y las columnas que se excluyen de un análisis adicional de los resultados de la exploración de descubrimientos de datos.

Exportado
Lista las tablas y columnas que se exportan después del análisis, y está listo para publicarse.

Descubrimiento basado en esquemas

Para bases de datos como, por ejemplo, Oracle, IBM Data Risk Manager proporciona un descubrimiento basado en esquemas. Al desencadenar la metaexploración, puede seleccionar los esquemas necesarios. Además, en el entorno de trabajo de limpieza, los activos se pueden agrupar basándose en el esquema.

Descubrimiento delta

Si se explora el mismo origen de datos para el descubrimiento, la parte delta de la tabla que se ha suprimido o añadido es visible en el entorno de trabajo de limpieza.

Descarga de resultados de limpieza de datos

Antes de exportar los resultados de limpieza a la taxonomía, puede crear un archivo CSV para que incluya los resultados de limpieza y descargar el archivo en una carpeta que elija.

Aplicación de reglas de filtrado

Aplique políticas y reglas a la base de datos seleccionada para incluir o excluir conjuntos de datos para el análisis.

Antes de empezar

- Asegúrese de que se importan los datos de contexto empresarial necesarios y que dispone de un programa con el ámbito adecuado para ejecutar la operación de descubrimiento de datos.
- Asegúrese de que las exploraciones de descubrimiento de datos para los orígenes de datos que están en el ámbito estén completas.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`) con privilegios de administrador.
2. Pulse el icono de menú  .
3. Seleccione un programa de la lista.
4. Vaya a **Centro de control y mandatos de seguridad** > **Análisis**.
5. En **Lista de bases de datos**, seleccione el origen de datos para el que necesita revisar los resultados de exploración.

   Cuando los resultados de descubrimiento de datos se cargan inicialmente, todos los datos, como las tablas y las columnas, se etiquetan como `Sin limpiar`.

   Si se completan los procesos de descubrimiento y clasificación en IBM Security Guardium, de forma predeterminada, se etiquetan los resultados en la política de IBM Security Guardium asociada.

6. Pulse **Añadir regla**. Se visualizarán las políticas de filtrado, que están definidas en la Central de gestión de políticas.
7. Seleccione una política de la lista.
8. Para incluir las reglas de política, seleccione **Inclusión**.
9. Para excluir las reglas de política, seleccione **Exclusión**.
10. Para aplicar el filtro basándose en la política seleccionada, pulse **Aplicar filtro**.

    Los elementos coincidentes se mostrarán en la sección **Etiquetado** en la página **Entorno de trabajo de análisis**.
11. Si tiene que excluir las columnas, aplique una regla de eliminación para eliminar los elementos de datos de su conjunto. Modifique la política asociada para que incluya una regla para eliminar los elementos de datos. Para obtener información sobre cómo modificar una política, consulte "Modificación de una política" en la página 137.
12. Pulse **Recuento de nivel** para ver la lista de políticas que se aplican. Puede revertir a una etapa anterior de limpieza, eliminando los filtros en cada nivel.
13. Repita los pasos para aplicar las políticas y reglas adecuadas para la inclusión o exclusión de acuerdo con sus requisitos de análisis.

Qué hacer a continuación

Exporte el conjunto filtrado de elementos de datos para la asignación y publicación de la taxonomía. Para obtener información sobre cómo exportar los resultados de análisis, consulte "Exportación de resultados de análisis de datos" en la página 146.

Exportación de resultados de análisis de datos

Exporte el conjunto filtrado de elementos de datos para la asignación y publicación de la taxonomía.

Antes de empezar

Asegúrese de que se hayan completado las tareas siguientes.

- La importación de los datos de contexto empresarial necesarios y la disponibilidad de un programa con el ámbito adecuado para ejecutar la operación de descubrimiento de datos.
- Las exploraciones de descubrimiento de datos para los orígenes de datos que están en el ámbito.
- La limpieza y el análisis de los resultados de exploración de descubrimientos de datos.

Procedimiento

1. Después de aplicar las reglas de política de filtrado necesarias, asegúrese de que los elementos coincidentes se visualizan en la sección **Etiquetado** en la página **Entorno de trabajo de análisis**.

   Las tablas y columnas para la base de datos seleccionada y las coincidencias adecuadas si se ha aplicado una política durante la exploración de clasificaciones, se visualizan para el análisis.
2. Para exportar el conjunto filtrado de elementos de datos, pulse el icono **Exportar a taxonomía**  .
3. Cuando se le solicite, pulse **Sí** para exportar los conjuntos de datos a la taxonomía.
4. Pulse el icono **Exportado** 

para ver las tablas exportadas.

Qué hacer a continuación

Vaya a **Centro de control y mandatos de seguridad** > **Taxonomía** para validar si la operación de exportación se ha realizado correctamente.

Correlación y publicación de taxonomías

Utilice el componente Centro de control y mandatos de seguridad (SC3) de IBM Data Risk Manager para aplicar una taxonomía a los activos de datos limpiados y publicar activos en el panel de control de IBM Data Risk Manager. El panel de control habilita el gobierno de información proporcionando visualización y gestión en una única consola unificadora que representa los riesgos potenciales de los activos empresariales confidenciales.

Características de correlación de taxonomías

- Puede exportar el activo de información recién descubierto a través de varios programas.
- Si existen varios activos de información en el origen de datos asociado en **Centro de control y mandatos de seguridad** > **Taxonomía** > **Activos descubiertos recientemente**, puede aplicar los mismos atributos de taxonomía a todos los activos y publicar el activo.
- Los activos de información publicados o listos para publicar en el panel de control se pueden retrotraer mediante la opción `Retrotraer`. Cuando utiliza la opción `Retrotraer`, los activos se mueven de nuevo al asistente de limpieza.

Correlación de taxonomías

Utilice el componente Centro de control y mandatos de seguridad (SC3) de IBM Data Risk Manager para aplicar una taxonomía a los activos de datos limpiados y publicar los activos en el panel de control de IBM Data Risk Manager.

Antes de empezar

Asegúrese de que se hayan completado las tareas siguientes.

- La importación de los datos de contexto empresarial necesarios y la disponibilidad de un programa con el ámbito adecuado para ejecutar la operación de descubrimiento de datos.
- Las exploraciones de descubrimiento de datos para los orígenes de datos que están en el ámbito.
- La limpieza y el análisis de los resultados de exploración de descubrimientos de datos.
- La exportación de activos de datos limpiados.

Acerca de esta tarea

- Puede exportar el activo de información recién descubierto a través de varios programas.
- Si existen varios activos de información en el origen de datos asociado en **Centro de control y mandatos de seguridad** > **Taxonomía** > **Activos descubiertos recientemente**, puede aplicar los mismos atributos de taxonomía a todos los activos y publicar el activo.
- Los activos de información publicados o listos para publicarlos en el panel de control se pueden retrotraer. Cuando se utiliza la opción **Retrotraer**, los activos se mueven de nuevo al asistente de limpieza.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://`*`<dirección-IP-servidor-IDRM>`*`:8443/albatross/a3suite`) con privilegios de administrador.
2. Pulse el icono de menú .
3. Seleccione un programa en el que desea correlacionar la taxonomía.
4. Vaya a **Centro de control y mandatos de seguridad** > **Taxonomía** > **Estructurados**.
5. Pulse el icono de menú desplegable y seleccione **Activos descubiertos recientemente**.

Se mostrarán los activos de datos limpiados exportados de **Centro de control y mandatos de seguridad** > **Análisis** > **Entorno de trabajo de análisis**.

6. Seleccione un origen de datos de la lista que desea publicar.
7. En la página **Activos descubiertos recientemente**, si se importan los datos de contexto, los atributos de taxonomía primarios y secundarios ya están correlacionados. Si es necesario, puede cambiar los atributos. Por ejemplo, puede cambiar los atributos de `Conformidad` y `Categoría`.

   Nota: Si los atributos de taxonomía no se correlacionan de forma automática, valide la correlación en **Modelador de contexto empresarial**.
8. En la sección **Atributos primarios**, puede utilizar etiquetas para identificar un grupo de activos de datos asociados. Puede:

   a. Cree etiquetas para definir las agrupaciones de activos de datos.

   b. Asocie un activo de datos a más de una etiqueta.

   Para crear una etiqueta:

   a. Pulse la lista desplegable **Etiqueta**.

   b. En el campo **Añadir nuevo nombre de etiqueta**, especifique un nombre para la etiqueta.

   c. Para guardar la etiqueta, pulse el icono Añadir  .

   Para aplicar etiquetas a un activo de datos:

   a. Pulse la lista desplegable **Etiqueta**.

   b. Seleccione las etiquetas de la lista.
9. Para convertir el activo en un activo de joya de la corona, habilite el botón de conmutador. Joya de la corona es un término que se utiliza para representar el activo de datos más valioso de una organización.
10. Asigne una valoración de confidencialidad, integridad y disponibilidad (CIA, por sus siglas en inglés Confidentiality Integrity Availability) para evaluar el riesgo del activo de información, 1 = bajo, 2 = medio y 3 = alto.
11. Pulse **Guardar** para guardar los cambios, si los hay.
12. Seleccione **Aplicar a todo** para aplicar los cambios a todos los activos descubiertos en el origen de datos actual.
13. Pulse **Retrotraer** si desea retrotraer un activo de información que está listo para su publicación en el panel de control. El activo de información se devuelve al asistente de limpieza para realizar los cambios necesarios.
14. Valide los activos de datos y pulse **Exportar**.
15. En la lista **Exportar**, seleccione los programas a los que desea publicar los activos.
16. Pulse **Exportar**.

    En la lista de activos publicados se mostrarán los activos de información bajo **Centro de control y mandatos de seguridad** > **Taxonomía** > **Activos de información**.
17. Para aplicar una taxonomía a los activos de datos sin estructurar, vaya a **Centro de control y mandatos de seguridad** > **Taxonomía** > **Sin estructurar**.
18. Repita los mismos pasos para aplicar la taxonomía y exportar los activos al panel de control según sea necesario.

Qué hacer a continuación

Verifique si el activo que ha exportado ahora es visible en el panel de control de IBM Data Risk Manager.

Utilización del panel de control para ver los datos de activos exportados

Utilice el panel de control de IBM Data Risk Manager para ver y analizar los datos del proceso de descubrimiento y clasificación. El panel de control habilita el gobierno de información proporcionando

visualización y gestión en una única consola unificadora que representa los riesgos potenciales de los activos empresariales confidenciales.

Antes de empezar

Asegúrese de que se hayan completado las tareas siguientes.

- La importación de los datos de contexto empresarial necesarios y la disponibilidad de un programa con el ámbito adecuado para ejecutar la operación de descubrimiento de datos.
- Las exploraciones de descubrimiento de datos para los orígenes de datos que están en el ámbito.
- La limpieza y el análisis de los resultados de exploración de descubrimientos de datos.
- La exportación de activos de datos limpiados.
- Aplicación de una taxonomía a los activos de datos limpiados y publicación de activos en el panel de control de IBM Data Risk Manager.Para obtener más información sobre el panel de control, consulte “Panel de control de IBM Data Risk Manager” en la página 177.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`) con privilegios de administrador.
2. Pulse el icono de menú .
3. Pulse **Panel de control**.
4. Seleccione el programa.
5. Pulse **Panel de control**.
6. En la página **Conjunto de activos de información**, pulse el icono de flecha en el activo para ver los detalles del activo.

   Se mostrará la ventana emergente **Detalles de activo**.

Diagramas de modelador

Puede utilizar el componente **IBM Data Risk Manager** > **Modelador de contexto empresarial** > **Modelador** para crear diagramas de flujo de contexto y diagramas de flujo de datos. Los diagramas de flujo de datos proporcionan una vista de ciclo de vida de los datos y su flujo a través de entidades organizativas clave que son más fáciles de entender para usuarios técnicos y no técnicos.

Crear un diagrama de modelador

Se puede crear un diagrama de modelo utilizando el componente IBM Data Risk Manager Modeler para comprender mejor las relaciones entre las distintas entidades de negocio de una organización como, por ejemplo, procesos de negocio, aplicaciones o infraestructura.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Modelador**.
4. Seleccione **Diagrama**.
5. Pulse el icono **Crear diagrama** .
6. En la ventana **Crear diagrama**, establezca las opciones siguientes y pulse **Crear**.

Opción	Descripción
Nombre de diagrama	El nombre del diagrama.
Unidad empresarial	Nombre de la unidad de negocio.
Propietario	El nombre del propietario.
Programa	El programa asociado al diagrama.
Tipo de diagrama	El tipo de diagrama, tal como `Contexto empresarial` o `Flujo de datos`.

Nota: Se muestra la lista de plantillas, si está disponible. Puede seleccionar la plantilla para crear sus diagramas de modelo.

7. Para seleccionar las entidades de datos de contexto, pulse el icono desplegable .
8. Seleccione una entidad en la lista, por ejemplo, `Aplicación`.
   Se muestran los atributos de la entidad de datos de contexto seleccionada bajo `Aplicación`.
9. Para crear el diagrama, arrastre y suelte los atributos necesarios en el área de diagrama, en función de sus preferencias.
10. Conecte las entidades utilizando los conectores apropiados y las opciones de dibujo disponibles en la barra de herramientas de dibujo.
11. Pulse en el enlace de conexión para añadirle texto que describa la relación.
12. Para guardar el diagrama, pulse el icono **Guardar diagrama** .
13. De forma alternativa, puede trazar automáticamente el diagrama.
    a) En el área de dibujo, en el atributo seleccionado, pulse en el icono de conexión automática .
    b) Seleccione los atributos necesarios en la lista, según sus necesidades.
    c) Pulse **Gráfico**.
    d) Para guardar el diagrama, pulse el icono **Guardar diagrama** .
14. Para abrir un diagrama existente, pulse en el icono **Abrir diagramas** .

Crear un diagrama de plantilla

Se pueden crear diagramas de plantilla utilizando el componente IBM Data Risk Manager Modeler. Se puede crear un diagrama de plantilla basado en las plantillas disponibles.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) con sus credenciales de usuario.
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Modelador**.
4. Seleccione **Plantilla**.
5. Pulse el icono Crear plantilla .
6. En la ventana **Crear plantilla**, especifique el nombre del diagrama.
7. Pulse **Crear**.
8. Para seleccionar las entidades de datos de contexto, pulse el icono desplegable .
9. Seleccione una entidad en la lista, por ejemplo, `Aplicación`.
   Se muestran los atributos de la entidad de datos de contexto seleccionada bajo `Aplicación`.

10. Para crear la plantilla, arrastre y suelte los atributos necesarios en el área de diagrama, en función de sus preferencias.
11. Conecte las entidades utilizando los conectores apropiados y las opciones de dibujo disponibles en la barra de herramientas de dibujo.
12. Pulse en el enlace de conexión para añadirle texto que describa la relación.
13. Para guardar la plantilla, pulse en el icono **Guardar plantilla** .
14. De forma alternativa, puede trazar automáticamente el diagrama de plantilla.
    a) En el panel de dibujo, en el atributo seleccionado, pulse el icono de conexión automática .
    b) Seleccione los atributos necesarios en la lista, según sus necesidades.
    c) Pulse **Gráfico**.
    d) Para guardar la plantilla, pulse en el icono **Guardar plantilla** .

Qué hacer a continuación
Las plantillas que ha creado se muestran en la ventana Crear diagrama. En la lista, puede seleccionar la plantilla para crear sus diagramas de modelo. Para ver los pasos sobre cómo crear un diagrama de modelo, consulte "Crear un diagrama de modelador" en la página 149.

Para abrir una plantilla existente, pulse en el icono **Abrir plantillas** .

Centro de acción

IBM Data Risk Manager proporciona la función de flujo de trabajo de reparación de vulnerabilidades y riesgos, que se puede utilizar para definir un plan de acción, enviarlo al propietario y realizar un seguimiento hasta el cierre.

Una vez que se hayan identificado los problemas de seguridad de datos y se haya evaluado el nivel de requisito de reparación, la organización debe seguir un proceso de gestión de reparaciones para abordar y gestionar los problemas. Puede utilizar el componente Centro de acción de IBM Data Risk Manager para gestionar planes de acción de reparación para las vulnerabilidades y los riesgos identificados. Las actividades de reparación se pueden definir para los elementos siguientes.

Orígenes de datos
En el componente Centro de acción, puede crear una actividad para un origen de datos específico del inventario de IBM Data Risk Manager para reparar los problemas identificados. Si los orígenes de datos se importan desde ServiceNow, puede utilizar ServiceNow para la gestión de reparaciones. Para obtener más información sobre cómo crear una actividad, consulte "Creación de una actividad de reparación " en la página 153.

Resultados de la prueba de evaluación de vulnerabilidades
En el componente Gestión de vulnerabilidades, puede asignar un conjunto de resultados de prueba de evaluación de vulnerabilidades erróneos como ámbito para crear una actividad de reparación. Para obtener más información sobre la creación de actividades, consulte "Creación de una actividad para reparar vulnerabilidades " en la página 48. Posteriormente, puede utilizar el Centro de acción para ver y gestionar estas actividades.

Riesgos de la evaluación
En el componente Evaluación, puede crear una actividad de reparación para los riesgos de evaluación que están asociados a ámbitos como, por ejemplo, aplicaciones, procesos de negocio u orígenes de datos. Para obtener más información sobre la creación de actividades, consulte "Creación de un plan de acción para reparar riesgos " en la página 202. Posteriormente, puede utilizar el Centro de acción para ver y gestionar estas actividades.

Actividades de reparación predefinidas

Puede añadir actividades de reparación predefinidas y las tareas importadas desde un paquete de soluciones para definir planes de acción en el Centro de acción. Para obtener más información sobre cómo añadir actividades predefinidas, consulte “Adición de tareas y actividades predefinidas ” en la página 156.

ServiceNow para la gestión de reparaciones

Puede utilizar la integración de IBM Data Risk Manager y ServiceNow para crear, actualizar y cerrar incidencias de ServiceNow para las actividades de reparación que se crean en el Centro de acción.

La integración de IBM Data Risk Manager y ServiceNow es una integración bidireccional que proporciona las funciones siguientes:

- Publica actividades de reparación que se crean para orígenes de datos de ServiceNow desde el Centro de acción para la instancia de ServiceNow como incidencias.
- Actualiza automáticamente el estado de la actividad o incidencia y otros detalles en el Centro de acción y, también, en ServiceNow. Si una actividad está cerrada en el Centro de acción, también se cierra la incidencia de ServiceNow correspondiente. Si la incidencia se resuelve en ServiceNow, también se cierra la actividad del Centro de acción correspondiente.

Visualización de detalles de actividad de proyecto y reparación

El panel de control de Centro de acción de IBM Data Risk Manager proporciona una visión general de los proyectos y las actividades bajo cada proyecto que están definidos para gestionar acciones de reparación en riesgos y vulnerabilidades identificados.

Acerca de esta tarea

En el Centro de acción, también puede ver y gestionar actividades de reparación para las vulnerabilidades que ha creado en el componente Gestión de vulnerabilidades y las acciones de reparación de riesgos que se han creado en el componente Evaluación de IBM Data Risk Manager. En el panel de control, puede ver la información siguiente.

- Lista de proyectos para un programa seleccionado.
- Lista de actividades bajo cada proyecto.
- Un estado general rápido de las actividades.
- Una fácil navegación a los proyectos y las actividades para visualizar detalles y para supervisar el estado.
- Una vista consolidada de comentarios de actividad y tareas.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Centro de acción** > **Programa** para seleccionar un programa.
4. En la página del panel de control, en **Proyectos**, se muestra la lista de proyectos. Seleccione un proyecto en la lista. Se muestran las actividades que se han definido para el proyecto seleccionado.
5. Para crear una actividad para un programa seleccionado bajo un proyecto, pulse el icono **Añadir actividad** .
6. Para añadir una actividad predefinida para un proyecto, pulse el icono de actividades predefinidas . Las actividades predefinidas para la reparación se importan desde los paquetes de soluciones.
7. Para una actividad seleccionada, puede ejecutar las operaciones siguientes.

- Para modificar detalles de actividad, pulse el icono editar  .
- Para ver tareas asociadas, pulse el icono de flecha hacia abajo en **Tareas**. Puede modificar el estado de la tarea y añadir un comentario a la tarea.
- Para ver ámbitos asociados, pulse el icono de flecha hacia abajo en **Ámbito**.
- Para modificar el estado de la actividad, pulse el icono de flecha hacia abajo en **Estado**. Si cambia el estado de la actividad a **Completada**, los estados de las tareas asociadas también se actualizan a **Completada**.
- Para ver y publicar un comentario, pulse el icono de comentarios  . La ventana **Comentarios de actividad** proporciona una vista consolidada de comentarios de actividad y comentarios de tarea.
- Para mostrar actividades en el panel de control basándose en los criterios seleccionados, pulse el icono de filtro para el **Nombre de actividad** o el **Estado**.

Creación de una actividad de reparación

Utilice el componente Centro de acción de IBM Data Risk Manager para crear una actividad de reparación sobre las vulnerabilidades identificadas en un origen de datos específico.

Antes de empezar

Para un origen de datos de ServiceNow, puede crear una actividad y publicarla como una incidencia sobre ServiceNow para la gestión de reparaciones. Actualmente, puede publicar la actividad solo en una única instancia de ServiceNow.

Para utilizar ServiceNow para la gestión de reparaciones, asegúrese de que IBM Data Risk Manager está integrado con ServiceNow. Para obtener más información sobre la integración, consulte “Integración de ServiceNow con IBM Data Risk Manager” en la página 74.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Centro de acción** > **Programa** para seleccionar un programa.
4. En la página del panel de control, pulse el icono **Añadir actividad**  .
5. En la ventana **Crear actividad con proyecto**, especifique un nombre de proyecto y un nombre de actividad. También puede seleccionar un proyecto existente y especificar un nombre de actividad.
6. Para crear una actividad de reparación de vulnerabilidad, pulse el icono **Reparación para evaluación de vulnerabilidades**  .
7. En la página **Actividad para la evaluación de vulnerabilidades**, especifique los valores necesarios para los **Campos primarios**.

Opción	Descripción
Estado	Especifique el estado de la actividad, por ejemplo, `Por iniciar`, `En curso` o `Completada`.
Seleccionar origen de datos	Seleccione un origen de datos en el inventario de orígenes de datos para el cual debe crear una actividad de reparación. Solo puede asignar un origen de datos como ámbito a una actividad.
Publicar en	Si selecciona el origen de datos de ServiceNow, puede publicar la actividad como incidencia en ServiceNow.

Opción	Descripción
	Para publicar, habilite el botón de conmutador de ServiceNow. Una vez que se haya publicado la actividad, puede ver el número de incidencia en la página del panel de control.
Operación de actividad	Seleccione una actividad de operación en la lista.
Fecha de inicio	Especifique la fecha para iniciar la actividad de reparación.
Fecha de finalización	Especifique la fecha para finalizar la actividad de reparación.
Duración	Especifica la duración entre la fecha de inicio y finalización de la actividad.

8. Especifique los valores necesarios para los **Campos secundarios**.

   Puede añadir elementos de lista a los campos secundarios como, por ejemplo, **Impacto**, **Urgencia**, **Prioridad**, **Subcategoría**, **Gravedad**, **Categoría** y **Tipo de contacto** creando un elemento de registro para los registros respectivos (campos) en el **Modelador de contexto empresarial** > **Creador de infraestructuras** > **Registrar definiciones**. Puede añadir una propiedad a un elemento de registro para correlacionar el campo de IBM Data Risk Manager con el campo de ServiceNow equivalente.

   Para ver los pasos sobre cómo crear un elemento de registro y añadir una propiedad, consulte "Crear un elemento y subelemento para el registro" en la página 187.
9. Para guardar los detalles de actividad, pulse **Guardar**.

Qué hacer a continuación
Defina la información de contexto necesaria para la actividad que acaba de crear. Pulse **Gestión de contexto** para definir información de contexto. Para obtener más información sobre la gestión de contexto, consulte "Definición de información de contexto para una actividad " en la página 154.

Definición de información de contexto para una actividad

Para la actividad de reparación que haya creado, añada la información de contexto apropiada que le ayuda a comprender mejora la actividad.

Acerca de esta tarea
Puede definir la información de contexto siguiente.

Ámbito de actividad
Los resultados fallidos de la exploración de evaluación de vulnerabilidades que se ejecuta en el origen de datos seleccionado están disponibles para asignarlos como ámbito a la actividad.

Tareas
Las taras describen elementos de trabajo que son necesarios para alcanzar el objetivo de una actividad de reparación. Las tareas tienen uno o más usuarios encuestados de tarea que son responsables de ejecutar la tarea dentro del periodo de tiempo especificado. Una actividad puede contener varias tareas.

Notificaciones
Las notificaciones permiten a los usuarios recibir avisos puntuales de actividades y tareas. Se puede enviar notificaciones a varios usuarios.

Comentario
Los comentarios proporcionan un lugar para añadir cualquier texto a la actividad. A menudo, los comentarios podrían ser información adicional, aclaraciones, opiniones, detalles o revisiones.

Procedimiento

1. Cree una actividad bajo un proyecto para el programa que seleccione. Para ver los pasos sobre cómo crear una actividad, consulte “Creación de una actividad de reparación ” en la página 153.
2. En la página **Actividad para evaluación de vulnerabilidades**, pulse el icono **Gestión de contexto** .
3. Asigne un ámbito a la actividad.
   a) Pulse **Ámbito de actividad**.
   b) Seleccione los resultados fallidos de la evaluación de vulnerabilidades necesaria como ámbito de actividad.
   c) Pulse **Guardar**.
4. Cree una tarea. Puede crear varias tareas para una actividad de reparación.
   a) Pulse **Tareas**.
   b) Establezca las opciones siguientes y pulse **Guardar**.

Opción	Descripción
Nombre de tarea	Especifique un nombre para la tarea.
Operación de la tarea	Seleccione una operación de tareas en la lista.
Estado	Especifique el estado de tarea actual como, por ejemplo, `Por iniciar`, `En curso` o `Completada`.
Fecha de inicio	Especifique la fecha para iniciar la tarea.
Fecha de finalización	Especifique la fecha para finalizar la tarea.
Recursos asignados	Asigne recursos para ejecutar la tarea. Puede seleccionar varios recursos.
Descripción	Añada más información para la tarea que ha creado.
Comentario	Añada comentarios sobre la tarea.

5. Añadir notificaciones
   a) Pulse **Notificaciones**.
   b) Establezca las opciones siguientes y pulse **Guardar**.

Opción	Descripción
Nombre de notificación	Especifique un nombre para la notificación.
Estado	Especifique el estado de la notificación para indicar si la notificación se ha enviado al usuario.
Fecha de inicio	Especifique la fecha de inicio.
Fecha de finalización	Especifique la fecha de finalización.
Recursos asignados	Asigne recursos para recibir la notificación. Puede seleccionar varios recursos.
Descripción	Añada más información sobre la notificación que está enviando.
Comentario	Añada comentarios en los comentarios sobre la notificación.

6. Añada un comentario para la actividad que ha creado.

a) Pulse **Comentario**.

b) Añada los comentarios.

c) Pulse **Publicar**.

d) Pulse **Guardar**.

7. Puede ver la actividad que ha creado ahora con su información de contexto asociada en la página del panel de control Centro de actividad.

Adición de tareas y actividades predefinidas

Puede utilizar actividades y tareas de reparación predefinidas que se importan desde un paquete de soluciones para definir planes de acción en el Centro de acción.

Antes de empezar

Asegúrese de que los paquetes de soluciones se hayan importado a IBM Data Risk Manager para utilizar las actividades y tareas predefinidas. Para obtener más información sobre el paquete de soluciones, consulte “Paquetes de soluciones” en la página 133.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Centro de acción** > **Programa** para seleccionar un programa.
4. En la página del panel de control Centro de acción, seleccione un proyecto en la lista **Proyectos**.
5. Pulse el icono de actividades predefinidas  .
6. En la ventana **Actividades predefinidas para la reparación**, seleccione las actividades necesarias.
7. Pulse el icono **Añadir actividad**  .
   Las actividades que ha añadido se listan en la página del panel de control.
8. Modifique los detalles de actividad basándose en los requisitos. Para modificar detalles de actividad, seleccione una actividad y pulse el icono de edición  .

Informe

Utilice la función de informe de IBM Data Risk Manager para generar informes y utilizarlos para fines de análisis y de negocios.

La protección de datos requiere la protección y el análisis continuos de los datos. IBM Data Risk Manager recopila una gran cantidad de datos de diversos orígenes para el análisis de riesgos. Puede ver estos datos en forma de informes con distintos formatos para ver y analizar los datos rápidamente. El motor de informes de IBM Data Risk Manager se utiliza para generar informes utilizando plantillas predefinidas para activos, inventario, evaluación y entorno de trabajo de análisis. Puede crear informes personalizados seleccionando columnas, aplicando filtros y ordenando cómo aparecen las columnas en el informe, a fin de que se ajusten a sus necesidades de negocio.

Plantillas de informes

IBM Data Risk Manager proporciona las siguientes plantillas de informe para crear un informe.

- Lista de activos con infraestructura
- Lista de activos de información con activos de datos

- Lista de activos de información
- Inventario de infraestructuras

Para obtener más información sobre las plantillas de informes de IBM Data Risk Manager, consulte “Plantillas de informes” en la página 157.

Formatos de informe

Los datos de informe generados se muestran en formato tabular. A continuación, puede descargar estos datos en un archivo de valores separados por comas (CSV). Descargue el informe para guardar los datos de informe en su disco duro, realizar análisis adicional o publicar el informe en otra aplicación.

Plantillas de informes

Las plantillas de informes son plantillas predefinidas para diferentes módulos en la aplicación. Las plantillas de informe de IBM Data Risk Manager le permiten crear sus propios informes con las métricas y los datos que desea ver.

IBM Data Risk Manager proporciona varias plantillas tal como se describen en las secciones siguientes para crear informes que ayudan a analizar datos y a tomar decisiones empresariales fundamentadas.

Lista de activos con infraestructura

La plantilla de informe proporciona detalles de los activos de información de IBM Data Risk Manager y de las infraestructuras asociadas. Puede utilizar la plantilla para mostrar los detalles de los widgets de Infraestructura y de Conjunto de activos de información del Panel de Control de IBM Data Risk Manager de un programa seleccionado.

Elementos de plantilla	Descripción
ID de activo	Identificador de activo exclusivo generado por sistema.
Nombre de activo	Nombre del activo de información.
Nombre de infraestructura	Nombre de la infraestructura.
ID de infraestructura	Identificador de infraestructura exclusivo generado por sistema.
Nivel de riesgo de infraestructura	Nivel de riesgo de la infraestructura. Por ejemplo, Alto (rojo), Medio (ámbar) o Bajo (verde) en función de criterios de puntuación predefinidos.
Nivel de riesgo de activo	Nivel de riesgo de los activos de información. Por ejemplo, Alto (rojo), Medio (ámbar) o Bajo (verde) en función de criterios de puntuación predefinidos.
Ubicación de la ciudad de infraestructura	Nombre de la ciudad donde se encuentra el origen de datos.
Ubicación del país de infraestructura	Nombre del país donde se encuentra el origen de datos.
Recuento de tablas	Número total de tablas de origen de datos que están asociadas al activo de información.
Recuento clasificado de infraestructuras	Número total de infraestructuras asociadas al activo de información.
Joya de la corona	Indica si el activo de información tiene información de joya de la corona del máximo valor, cuyo comprometimiento tendría un impacto empresarial de primer orden.
Dirección IP	Dirección IP del servidor donde reside el origen de datos.

Elementos de plantilla	Descripción
Nombre de host	Nombre de host del servidor del origen de datos.
Recuento de vulnerabilidades de infraestructura	Recuento total de vulnerabilidades de infraestructura asociadas a los puntos finales o servidores.
Categoría del activo	Categorías de clasificación de datos en términos de la necesidad de protección como, por ejemplo, Públicamente Disponible, Internamente controlado, Confidencial PII, Confidencial de empresa, Altamente Confidencial/Restringido, Público, Solo Para Uso Oficial, o Confidencial.
Conformidad de activos	Obligaciones normativas asociadas al activo como, por ejemplo, HIPAA, SOX o PCI.
Recuento de columnas	Número total de columnas de tabla de origen de datos asociadas al activo de información.
Nombre del programa	Nombre del programa al que está asociado el activo de información.
Conformidad	Obligaciones normativas asociadas al activo como, por ejemplo, HIPAA, SOX o PCI.
Confidencialidad	Puntuación de Disponibilidad de Integridad de Confidencialidad (Confidentiality Integrity Availability, CIA) que representa el nivel de confidencialidad de los activos de información como, por ejemplo, 1 = bajo, 2 = medio y 3 = alto.
Etiqueta	Nombre de etiqueta que identifica un grupo de activos de información asociados.

Lista de activos de información con activos de datos

La plantilla de informe proporciona detalles de los activos de información de IBM Data Risk Manager y de los activos de datos asociados. La plantilla se puede usar para mostrar los detalles del widget Conjunto de activos de información de IBM Data Risk Manager junto con los datos de la sección Visión general de la página secundaria Conjunto de activos de información de un programa seleccionado.

Elementos de la plantilla	Descripción
Nombre clasificado	Nombre de las tablas de origen de datos asociadas al activo de información.
Columna clasificada	Nombres de columna de tabla del origen de datos asociados al activo de información.
ID de activo	Identificador de activo exclusivo generado por sistema.
Nombre de activo	Nombre del activo de información.
Nombre de infraestructura	Nombre de la infraestructura asociada al activo de información.
Dirección IP	Dirección IP del servidor donde reside el origen de datos.
Nombre de host	Nombre de host del servidor del origen de datos.
Etiqueta	Nombre de etiqueta que identifica un grupo de activos de información asociados.
Nombre del programa	Nombre del programa al que está asociado el activo de información.

Elementos de la plantilla	Descripción
Joya de la corona	Indica si el activo de información tiene información de joya de la corona del máximo valor, cuyo comprometimiento tendría un impacto empresarial de primer orden.
Confidencialidad	Puntuación de Disponibilidad de Integridad de Confidencialidad (Confidentiality Integrity Availability, CIA) que representa el nivel de confidencialidad de los activos de información como, por ejemplo, 1 = bajo, 2 = medio y 3 = alto.
Conformidad	Obligaciones normativas asociadas al activo como, por ejemplo, HIPAA, SOX o PCI.

Lista de activos de información

La plantilla de informe proporciona detalles de los activos de información de IBM Data Risk Manager. La plantilla se puede usar para mostrar los detalles del widget Conjunto de activos de información del Panel de Control de IBM Data Risk Manager de un programa seleccionado.

Elementos de la plantilla	Descripción
Nombre	Nombre del activo de información.
ID	Identificador de activo exclusivo generado por sistema.
Categoría	Categorías de clasificación de datos en términos de la necesidad de protección como, por ejemplo, Públicamente Disponible, Internamente controlado, Confidencial PII, Confidencial de empresa, Altamente Confidencial/Restringido, Público, Solo Para Uso Oficial, o Confidencial.
Tipo	Tipo de activo de datos como, por ejemplo, Activo de información.
Joya de la corona	Indica si el activo de información tiene información de joya de la corona del máximo valor, cuyo comprometimiento tendría un impacto empresarial de primer orden.
Confidencialidad	Puntuación de Disponibilidad de Integridad de Confidencialidad (Confidentiality Integrity Availability, CIA) que representa el nivel de confidencialidad de los activos de información como, por ejemplo, 1 = bajo, 2 = medio y 3 = alto.
Conformidad	Obligaciones normativas asociadas al activo como, por ejemplo, HIPAA, SOX o PCI.
Nivel de riesgo	Nivel de riesgo de los activos de información. Por ejemplo, Alto (rojo), Medio (ámbar) o Bajo (verde) en función de criterios de puntuación predefinidos.
Motivo del riesgo	Razones de los niveles de riesgo de los activos de información.
Etiqueta	Nombre de etiqueta que identifica un grupo de activos de información asociados.
Nombre del programa	Nombre del programa al que está asociado el activo de información.

Inventario de infraestructuras

La plantilla de informe proporciona detalles del inventario de orígenes de datos de IBM Data Risk Manager.

Elementos de la plantilla	Descripción
Nombre de infraestructura	Nombre del origen de datos en el inventario de IBM Data Risk Manager.
Plataforma	Nombre del servidor de base de datos en el que se ha creado el origen de datos.
Dirección IP	Dirección IP del servidor donde reside el origen de datos.
Host	Nombre de host del servidor del origen de datos.
Recuento total de tablas	Número total de tablas de origen de datos.
Recuento de filas	Recuento de filas de la tabla.
Recuento total de activos	Número total de activos de información a los que está asociado el origen de datos.
Ciudad	Nombre de la ciudad donde se encuentra el origen de datos.
País	Nombre del país donde se encuentra el origen de datos.
Clasificado	La clasificación de seguridad de los activos de información.
Infraestructuras con joya de la corona	Indica si el activo de información tiene información de joya de la corona del máximo valor, cuyo comprometimiento tendría un impacto empresarial de primer orden.
Infraestructura con datos confidenciales	Indica si el activo tiene datos confidenciales. El nivel de sensibilidad de los activos de datos se representa proporcionando una puntuación del nivel de Disponibilidad de Integridad de Confidencialidad (Confidentiality Integrity Availability, CIA) como, por ejemplo, 1 = bajo, 2 = medio y 3 = alto.
Recuento de vulnerabilidades pasadas	Número de exploraciones de vulnerabilidad pasadas.
Recuento de vulnerabilidades fallidas	Número de exploraciones de vulnerabilidad fallidas.
Supervisada	Indica si las actividades de base de datos se supervisan.
Cifrado	Indica el estado de cifrado de los orígenes de datos. Debe configurar IBM Data Risk Manager para conectarse e interactuar con IBM Multi-Cloud Data Encryption para captar detalles de cifrado de orígenes de datos añadidos al inventario de distintos orígenes donde está desplegado el agente de IBM Multi-Cloud Data Encryption para el cifrado de datos.
Recuento de violaciones	Número de infracciones de política de la infraestructura.
Origen creado	Nombre del origen en el que se crea el origen de datos. Por ejemplo, ServiceNow.

Crear y guardar informes

Utilice la función de informe de IBM Data Risk Manager definiendo una serie de instrucciones para extraer información especifica para ayudarle a ver y analizar datos rápidamente.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Pulse **Informe**.
4. Pulse el icono **Nuevo informe**  .
5. En la página **Crear informe**, seleccione una plantilla para su informe.
6. Pulse **Siguiente**.
7. En **Valores generales**, especifique el nombre y la descripción del informe en los campos **Nombre** y **Descripción**.
8. Pulse **Siguiente**.
9. En **Valores de tabla**, ejecute los pasos siguientes.
   a) Pulse **Seleccionar columnas** para añadir columnas al informe. Los nombres de columna se muestran según la plantilla de informe seleccionada.
   b) Pulse **Aplicar filtro** para seleccionar la columna de filtro de los datos del informe.
   c) Pulse **Ordenar columnas** para definir el orden de clasificación de los campos de columna aplicables en el informe. Puede ordenar las columnas en orden **Ascendente** o **Descendente**.
10. Para guardar el informe, pulse **Guardar informe**.

    El informe que ha guardado se muestra en la sección **Lista de informes globales** para poder acceder a él más adelante.
11. De forma alternativa, pulse **Ejecutar ahora** para guardar y ver de forma inmediata los datos del informe.

Qué hacer a continuación

Puede ejecutar el informe posteriormente y ver los datos de informe en formato tabular, que se puede exportar a un archivo CSV. Para ver los pasos sobre cómo ejecutar un informe, consulte "Ejecución de un informe guardado" en la página 161.

Ejecución de un informe guardado

Cuando es necesario, se pueden ejecutar las definiciones de informe guardadas para ver los datos de informe. Si el informe contiene parámetros, se pueden definir los valores que interesen cada vez que se ejecute el informe.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) utilizando sus credenciales.
2. Pulse el icono de menú de aplicación  .
3. Pulse **Informe**.
4. En la sección **Lista de informes globales**, seleccione el informe que desea ejecutar.
5. Pulse en el icono **Ejecutar ahora**  .
6. En la ventana **Seleccionar parámetros**, seleccione los parámetros para los atributos seleccionados para filtrar los datos de informe.
7. Pulse **Ejecutar**.

   Los datos de informe generados se muestran en formato tabular. A continuación, puede exportar los datos a un archivo CSV.

Qué hacer a continuación
Puede exportar los datos de informe a un archivo CSV. Para ver los pasos sobre cómo exportar datos de informe, consulte “Descargar datos de informe a un archivo CSV” en la página 162.

Descargar datos de informe a un archivo CSV

Los datos de informe generados se muestran en formato tabular. A continuación, puede descargar estos datos en un archivo de valores separados por comas (CSV). Descargue el informe para guardar los datos de informe en su disco duro, realizar análisis adicional o publicar el informe en otra aplicación.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) utilizando sus credenciales de usuario.
2. Pulse el icono de menú de aplicación .
3. Pulse **Informe**.
4. Seleccione el informe que desea descargar de **Lista de informes globales**. De forma predeterminada, los datos del informe última ejecución se visualizan en formato tabular.

   Para seleccionar un informe ejecutado previamente, siga los pasos siguientes:

   a. Pulse en el icono **Historial de ejecución de informes** . Aparecerá la lista de informes ejecutados anteriormente.
   b. Seleccione un informe de la lista.

5. Para descargar los datos de informe en un archivo CSV, pulse en el icono **Descargar informe** .
6. Para abrir el archivo y guardarlo en la carpeta que se elija, pulse en el nombre del archivo CSV descargado que aparece en la esquina inferior izquierda de la página.

Edición de informes

Puede modificar los informes generados en IBM Data Risk Manager. Por ejemplo, es posible que deba añadir columnas nuevas y filtrar las condiciones para que el informe se ajuste a sus necesidades de negocio.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) utilizando sus credenciales de usuario.
2. Pulse el icono de menú de aplicación .
3. Vaya a **Informe**.
   Los informes guardados se muestran en la **Lista de informes globales**.
4. En la sección **Lista de informes globales**, seleccione el informe que desea editar.
5. Pulse en el icono **Editar** .
6. Realice los cambios necesarios.
7. Pulse **Guardar informe**.

Planificador de IBM Data Risk Manager

Utilice la función Planificador de IBM Data Risk Manager para crear y gestionar trabajos de ejecución automática de varias transacciones en los intervalos que defina.

El trabajo es un planificador basado en tiempo que ejecuta las tareas predefinidas en el servidor en una determinada instancia sin necesidad intervención administrativa. La ejecución de los trabajos planificados mantiene los datos del servidor de IBM Data Risk Manager sincronizados con los datos del servidor integrado. Con el Planificador de IBM Data Risk Manager, se pueden crear trabajos planificados para ejecutar los procesos siguientes.

Cargar exploraciones de evaluación de vulnerabilidades
Transacción para crear los trabajos planificados que descargan exploraciones de evaluación de vulnerabilidades del adaptador de integración que se especifique. Por ejemplo, se pueden descargar exploraciones de evaluación de vulnerabilidad de IBM Security Guardium, IBM QRadar Security Intelligence Platform y IBM Security AppScan Enterprise.

Cargar resultados de exploración de evaluación de vulnerabilidades
Transacción para crear los trabajos planificados para descargar resultados de exploraciones de evaluación de vulnerabilidades desde el adaptador de integración que se especifique. Por ejemplo, puede descargar los resultados de la exploración de evaluación de vulnerabilidades desde IBM Security Guardium Analyzer.

Obtener estado de supervisión
Transacción para crear los trabajos planificados que obtienen el estado de supervisión del nodo de infraestructura. Por ejemplo, se puede obtener el estado de supervisión de los nodos de infraestructura desde IBM Security Guardium y IBM Multi-Cloud Data Encryption.

Obtener inventario y riesgos
Transacción para crear los trabajos planificados que importan riesgos y datos de inventario del adaptador de integración que se especifique. Por ejemplo, se pueden importar datos de inventario e información de riesgo de OneTrust.

Visualización de detalles de trabajo y transacción

La página **Consola de planificador** proporciona una vista general de los trabajos planificados definidos para varias transacciones.

Acerca de esta tarea

Puede obtener y ver los detalles siguientes.

- Lista de transacciones y los trabajos planificados asociados.
- Estado global rápido de los trabajos planificados.
- Navegación fácil a los trabajos y transacciones para ver los detalles y supervisar el estado.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Planificador**. Se mostrará la página **Consola de planificador**.
4. En **Lista de transacciones**, se muestra la lista de transacciones. Seleccione una transacción de la lista. Los trabajos planificados definidos para la transacción seleccionada se muestran en **Detalles de trabajo** para visualizar detalles.
5. Para añadir un trabajo, pulse el icono **Añadir trabajo**  .
6. En un trabajo seleccionado, se pueden ejecutar las tareas siguientes:
   - Para modificar los detalles del trabajo, pulse en el icono **Editar**  .
   - Para suprimir un trabajo, pulse el icono **Suprimir**  .

- Para ver el historial de ejecuciones del trabajo, pulse en el icono **Historial**  .
- Para habilitar o inhabilitar un trabajo, pulse en el botón de conmutar  .

Adición de un trabajo planificado

Añada trabajos para ejecutar varias transacciones automáticamente en intervalos predefinidos. Por ejemplo, la adición de trabajos para descargar exploraciones de evaluación de vulnerabilidad, descargar resultados de exploraciones de evaluación de vulnerabilidad, obtener el estado de supervisión de nodos de infraestructura o importar datos de inventario y riesgos.

Antes de empezar

Asegúrese de que IBM Data Risk Manager esté integrado con el servidor de integración desde el que necesite importar los datos. Puede obtener los detalles de configuración consultando "Integraciones entre productos" en la página 34.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Planificador**.
4. En **Lista de transacciones**, seleccione la transacción para la que necesite añadir un trabajo.
5. En la página **Consola del planificador**, pulse el icono **Añadir trabajos**  .
6. En la ventana **Crear trabajo**, configure las opciones siguientes.

Opción	Descripción
Nombre del trabajo	Especifique el nombre del trabajo que está añadiendo.
Adaptadores	Especifique el nombre de instancia del adaptador de integración desde el que se importarán los datos.
Parámetros del trabajo	En las instancias de IBM Security Guardium, especifique la fecha del parámetro **Fecha de inicio**. Seleccione **Actualizable** para incrementar el parámetro de fecha de cada ejecución.

7. Pulse **Siguiente**.

Qué hacer a continuación

Hay que definir planificaciones al trabajo añadido. Para obtener los pasos de configuración de la planificación, consulte "Configuración de un trabajo planificado" en la página 164.

Configuración de un trabajo planificado

Los trabajos planificados se ejecutan automáticamente en un intervalo fijo en el servidor. Puede definir planificaciones para los trabajos creados con IBM Data Risk Manager Scheduler.

Antes de empezar

Asegúrese de que el trabajo se ha creado en IBM Data Risk Manager Scheduler.

Cuando se crea un trabajo con IBM Data Risk Manager Scheduler, las planificaciones de los trabajos se comparan con las planificaciones de los trabajos existentes de tipos similares. Hay que tener en cuenta las condiciones siguientes a la hora de planificar un trabajo.

Cargar exploraciones de evaluación de vulnerabilidades
La hora de inicio del nuevo trabajo no puede estar comprendida entre 60 minutos antes ni después de la hora de inicio del trabajo existente. Por ejemplo, si un trabajo de descarga de exploración existente se ha planificado para ejecutarse a las 3 AM, debe planificar el nuevo trabajo para que se ejecute antes de las 2 AM o después de las 4 AM.

Cargar resultados de exploración de evaluación de vulnerabilidades
La hora de inicio del nuevo trabajo no puede estar comprendida entre 60 minutos antes ni después de la hora de inicio del trabajo existente.

Obtener estado de supervisión
La hora de inicio del nuevo trabajo no puede estar comprendida entre 60 minutos antes ni después de la hora de inicio del trabajo existente.

Obtener inventario y riesgos
La hora de inicio del nuevo trabajo no puede estar comprendida entre 60 minutos antes ni después de la hora de inicio del trabajo existente.

Procedimiento

1. Cree un trabajo. Para ver los pasos sobre cómo crear un trabajo, consulte "Adición de un trabajo planificado" en la página 164.
2. Los trabajos planificados se pueden configurar para ejecutar por minuto, cada hora, cada semana, cada mes o cualquier combinación de las opciones anteriores. En la ventana **Planificación**, defina la fecha y hora de la ejecución del trabajo conforme a sus necesidades de negocio.
3. Pulse **Guardar**.
   El trabajo añadido aparece en la páginca **Detalles del trabajo**.

Gestión de vulnerabilidades

Puede utilizar el componente Gestión e vulnerabilidades de IBM Data Risk Manager para crear y activar una exploración para ayudarle a identificar de forma eficaz las vulnerabilidades en las bases de datos, puntos finales y aplicaciones. Después de que las exploraciones hayan identificado las vulnerabilidades, puede buscar y revisar datos de vulnerabilidad, reparar vulnerabilidades y volver a ejecutar las exploraciones para evaluar el nuevo nivel de riesgo.

Crear y activar una exploración de evaluación de vulnerabilidades

Utilice el componente Gestión de vulnerabilidades de IBM Data Risk Manager para crear y ejecutar la exploración de evaluación en IBM Security Guardium para identificar vulnerabilidades en bases de datos.

Antes de empezar
Asegúrese de que IBM Data Risk Manager está integrado con IBM Security Guardium. Para obtener más información sobre la integración, consulte "Integración de IBM Security Guardium con IBM Data Risk Manager" en la página 38.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Pulse **Gestión de vulnerabilidades**.
4. Seleccione un programa de la lista.
5. Pulse **Crear nueva evaluación**.
6. En la página **Crear nueva evaluación**, establezca las opciones siguientes y pulse **Crear evaluación**.

Opción	Descripción
Nombre de evaluación	Nombre de la evaluación de vulnerabilidades de IBM Security Guardium.
Tipo de exploración	El tipo de exploración, por ejemplo, `Explorador de base de datos`.
Plataforma	Selección de tipo de base de datos para ejecutar el proceso de evaluación de vulnerabilidades.
Ejecutar el	Instancia del adaptador de IBM Security Guardium para ejecutar el proceso de evaluación de vulnerabilidades. La lista solo contiene las instancias para las cuales está seleccionada la opción **Ejecutar VA** cuando se crea la instancia de integración.

7. En **Ámbito de evaluación**, añada orígenes de datos a la transacción en función del ámbito o de los últimos días de exploración. Puede añadir varios orígenes de datos.
8. Pulse **Añadir ámbito a transacción**.
9. Seleccione las pruebas de vulnerabilidad en la lista y pulse **Guardar**.
10. En **Transacciones pendientes** en la vista Transacción, pulse el icono **Iniciar proceso**  .
11. Seleccione **Explorar ahora**.

    Para planificar la exploración más tarde, seleccione **Explorar después**.

    Para guardar los detalles de la transacción tras la finalización del proceso en **Transacciones pendientes** para su reutilización, seleccione **Réplica**.
12. Para iniciar el proceso, pulse el icono **Activar evaluación**  .

Crear y activar una exploración de evaluación de puntos finales

Utilice el componente Evaluación de vulnerabilidades de IBM Data Risk Manager para crear y ejecutar la exploración de evaluación en IBM QRadar Security Intelligence Platform para identificar las vulnerabilidades de punto final.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM QRadar Security Intelligence Platform. Para obtener más información sobre la integración, consulte "Integración de IBM QRadar Security Intelligence Platform con IBM Data Risk Manager" en la página 54.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Pulse **Gestión de vulnerabilidades**.
4. Seleccione un programa de la lista.
5. Pulse **Crear nueva evaluación**.
6. En la página **Crear nueva evaluación**, establezca las opciones siguientes y pulse **Crear evaluación**.

Opción	Descripción
Nombre de evaluación	Nombre de la evaluación de puntos finales de IBM QRadar Security Intelligence Platform.
Tipo de exploración	El tipo de exploración, por ejemplo, `Explorador de vulnerabilidades del servidor`.

Opción	Descripción
Ejecutar el	Instancia del adaptador de IBM QRadar Security Intelligence Platform para ejecutar el proceso de evaluación de vulnerabilidades.

7. En **Ámbito de evaluación**, añada orígenes de datos a la transacción en función del ámbito o de los últimos días de exploración. Puede añadir varios orígenes de datos.
8. Pulse **Añadir ámbito a transacción**.
9. En **Transacciones pendientes** en la vista Transacción, pulse el icono **Iniciar proceso**  .
10. Seleccione **Explorar ahora**.

    Para planificar la exploración más tarde, seleccione **Explorar después**.

    Para guardar los detalles de la transacción tras la finalización del proceso en **Transacciones pendientes** para su reutilización, seleccione **Réplica**.
11. Para ejecutar el proceso, pulse el icono **Activar evaluación**  .

Crear y activar una evaluación de aplicaciones

Utilice el componente Gestión de vulnerabilidades de IBM Data Risk Manager para crear y ejecutar la exploración de evaluación en IBM Security AppScan Enterprise para identificar las vulnerabilidades de aplicaciones.

Antes de empezar

Asegúrese de que IBM Data Risk Manager está integrado con IBM Security AppScan Enterprise. Para obtener información sobre la integración, consulte "Integración de IBM Security AppScan Enterprise con IBM Data Risk Manager" en la página 62.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Pulse **Gestión de vulnerabilidades**.
4. Seleccione un programa de la lista.
5. Pulse **Crear nueva evaluación**.
6. En la página **Crear nueva evaluación**, establezca las opciones siguientes y pulse **Crear evaluación**.

Opción	Descripción
Nombre de evaluación	Nombre de la evaluación de aplicaciones de IBM Security AppScan Enterprise.
Tipo de exploración	El tipo de exploración, por ejemplo, `Explorador de aplicaciones`.
Ejecutar el	Instancia del adaptador de IBM Security AppScan Enterprise donde se ejecutará el proceso de evaluación.

7. En **Ámbito de evaluación**, añada orígenes de datos a la transacción en función del ámbito o de los últimos días de exploración. Solo se puede añadir un origen de datos al ámbito de la transacción.
8. Pulse **Añadir ámbito a transacción**.
9. Seleccione la prueba de vulnerabilidad en la lista y pulse **Guardar**.
10. En **Transacciones pendientes** en la vista Transacción, pulse el icono **Iniciar proceso**  .
11. Seleccione **Explorar ahora**.

Para planificar la exploración más tarde, seleccione **Explorar después** y especifique la hora a la que se debe ejecutar la exploración.

Para guardar los detalles de la transacción tras la finalización del proceso en **Transacciones pendientes** para su reutilización, seleccione **Réplica**.

12. Para iniciar el proceso, pulse el icono **Activar evaluación** .

Visualización de resultados de exploración

Utilice el componente Gestión de vulnerabilidades de IBM Data Risk Manager para ver los resultados de la exploración de la evaluación de vulnerabilidades para un análisis y acciones adicionales. La revisión de los datos ayuda a identificar problemas que puede abordar para mejorar la postura de seguridad de la organización.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Pulse **Gestión de vulnerabilidades**.
4. Pulse **Ver resultados**.
5. Pulse el icono de filtro en **Orígenes de datos VA** y seleccione un tipo de adaptador, por ejemplo, `IBM QRadar`.
6. Para un origen de datos seleccionado, pulse el número para **Aprobado**, **Error** u **Otros** para mostrar los resultados en la página **Resultados de prueba de vulnerabilidades**.

Creación de una actividad para reparar vulnerabilidades

Utilice el componente Gestión de vulnerabilidades de IBM Data Risk Manager para ver y reparar vulnerabilidades. Cuando se identifican las vulnerabilidades mediante exploraciones, se deben llevar a cabo acciones de reparación para evaluar la exposición de riesgo correcta para el activo de información.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Pulse **Gestión de vulnerabilidades**.
4. Vaya a **Vista de resultados**.
5. Pulse **Orígenes de datos VA**.
6. Pulse el icono de filtro en **Orígenes de datos VA** y seleccione el tipo de adaptador, por ejemplo, `IBM QRadar`.
7. De forma alternativa, puede seleccionar un origen de datos basado en la plataforma.
   a) Pulse **Plataformas VA**.
   b) Seleccione una plataforma y pulse el icono de base de datos para seleccionar el origen de datos.
8. Para un origen de datos seleccionado, pulse el número para **Error** para mostrar los resultados en la página **Resultados de la prueba de vulnerabilidades**.
9. Pulse el icono de flecha hacia abajo para seleccionar el nivel de gravedad.

10. Pulse el icono **Reparación** .
11. Pulse **Sí** para crear acciones de reparación.
12. En la ventana **Crear actividad de reparación**, especifique la información necesaria. Si el origen de datos procede de ServiceNow, puede publicar la actividad como incidencia en ServiceNow para la gestión de reparaciones.
13. Pulse **Crear**.

    En la página **Resultados de la prueba de vulnerabilidades**, en **Actividad**, puede ver los detalles de actividad si la fecha de finalización de la actividad es mayor que la fecha de ejecución de los resultados de prueba.

Qué hacer a continuación

Puede ver y gestionar las actividades de reparación que ha definido en las áreas siguientes.

Centro de acción de IBM Data Risk Manager

- Pulse el icono de menú de aplicación .
- Pulse **Centro de acción**.

Para obtener más información sobre el Centro de acción, consulte "Centro de acción" en la página 151.

La ventana Detalles de activo en el panel de control de IBM Data Risk Manager

- Pulse el icono de menú de aplicación .
- Pulse **Panel de control**.
- En la ventana **Conjunto de activos de información**, pulse el icono de flecha en el activo para ver los detalles del activo.
- En la ventana **Detalles de activo**, pulse **Infraestructura** > **Vulnerabilidades**.
- Para ver elementos de acción, seleccione el nodo de infraestructura y pulse **Elementos de acción**.

Modelado y visualización de riesgos

Utilice IBM Data Risk Manager para evaluar los riesgos que están asociados a los activos de datos confidenciales de una organización. A continuación, puede visualizar los riesgos en el panel de control de IBM Data Risk Manager para llevar a cabo las acciones necesarias para proteger su negocio.

IBM Data Risk Manager evalúa el riesgo basándose en una combinación de la naturaleza intrínseca de los activos de datos y distintos vectores de riesgo de infraestructura. La naturaleza intrínseca de los activos de datos hace referencia a las propiedades aplicables como, por ejemplo, la sensibilidad de los activos de datos, el nivel de clasificación de los activos de datos, o si un activo de datos tiene características especiales como, por ejemplo, una asociación con obligaciones legales o basadas en políticas. Los vectores de infraestructura hacen referencia a las vulnerabilidades, eventos y riesgos de evaluación que están asociados a una infraestructura que contiene activos de datos.

Niveles de riesgo

IBM Data Risk Manager utiliza una escala de tres puntos cuando se evalúan riesgos.

`Alto` [rojo]	Si un activo de datos se ha evaluado como en `Alto` riesgo, las oportunidades de infracción o la magnitud de potencial de infracción es alta. Se necesitan acciones correctivas inmediatas.

Medio [ámbar]	Si un activo de datos se ha evaluado como en riesgo Medio, las oportunidades de infracción o la magnitud de potencial de infracción es media. Se necesitan acciones correctivas dentro de un plazo razonable.
Bajo [verde]	Si un activo de datos se ha evaluado como en Bajo riesgo, las oportunidades de infracción o la magnitud de infracción potencial es media. No son necesarias acciones correctivas.

Factores y puntuación de riesgo

Los factores de riesgo y los datos de telemetría asociados a los factores de riesgo se acumulan de una forma, que puede asimilarse mediante el motor analítico de riesgos de IBM Data Risk Manager.

IBM Data Risk Manager tiene en cuenta los factores que están descritos en las secciones siguientes para evaluar automáticamente el riesgo del activo de información en un programa seleccionado.

Riesgos debidos a atributos inherentes del activo de datos

En IBM Data Risk Manager, los atributos siguientes determinan el valor inherente de los activos de datos. Una puntuación compuesta de los atributos forma la base para determinar los riesgos de los activos de información.

Información vital
Representa el activo de datos más valioso dentro de una organización. Por lo general, una organización no posee más del 2 % del volumen total de datos.

Categoría
Representa las categorías de activos de datos definidas en IBM Data Risk Manager.

- Disponible públicamente
- Controlado internamente
- Información de identificación personal confidencial
- Confidencial de la empresa
- Altamente confidencial/restringido
- Público
- Solo uso oficial
- Confidencial

Conformidad
Representa las obligaciones reglamentarias asociadas al activo de datos.

Nivel de sensibilidad
Indica los requisitos de confidencialidad, integridad y disponibilidad para el activo de datos.

Riesgos de infraestructura

Los riesgos de infraestructura son una indicación de la posición de seguridad de las plataformas de infraestructura subyacentes. Los activos de datos se encuentran en elementos de infraestructura como, por ejemplo, bases de datos o servidores de archivos.

Los vectores de riesgo siguientes se tienen en cuenta para calcular los riesgos de infraestructura.

Riesgos de obligatoriedad
Los riesgos de obligatoriedad de la infraestructura se evalúan basándose en los controles siguientes.

- Cifrado
- Supervisión
- Ejecución de la exploración de vulnerabilidades

Riesgos de vulnerabilidades

Las exploraciones de evaluación de vulnerabilidades se ejecutan periódicamente para identificar problemas de seguridad. Puede activar una exploración de vulnerabilidades desde IBM Data Risk Manager o importar de varios orígenes para identificar vulnerabilidades. Los riesgos de vulnerabilidades se evalúan basándose en la ponderación combinada de los factores de riesgo siguientes.

- Gravedad y recuento de las vulnerabilidades que se han descubierto.
- Estado de las acciones de reparación.

Riesgos de supervisión

Las amenazas se registran en el servidor syslog (sucesos de alertas) de varios servidores de integración que se han configurado con IBM Data Risk Manager. Los riesgos de supervisión se evalúan basándose en la ponderación combinada de los factores de riesgo siguientes.

- Gravedad y recuento de las alertas que se han registrado.
- Estado de las acciones de reparación.

Riesgos cualitativos

El análisis de riesgos cualitativos evalúa y documenta la probabilidad y el impacto de los riesgos de evaluación con respecto a una escala predefinida. Los riesgos de evaluación y los riesgos de IBM Data Risk Manager se evalúan basándose en la ponderación combinada de los factores de riesgo siguientes.

- Gravedad y recuento de los riesgos.
- Estado de las acciones de reparación.
- Estado de los riesgos.

Participación

La participación de un nodo de infraestructura en un activo de información determina la contribución del nodo a la puntuación de riesgo. La participación se determina como un porcentaje de los elementos de datos, que es aportado por el nodo al activo de información.

Visualización de riesgos mediante IBM Data Risk Manager

IBM Data Risk Manager proporciona vistas completas y dinámicas de los riesgos empresariales relacionados con los datos a los líderes de negocio. Un panel de control de riesgo empresarial intuitivo y un centro de control permiten descubrir, analizar y visualizar los riesgos a fin de adoptar las medidas adecuadas para proteger el negocio.

IBM Data Risk Manager proporciona visibilidad multinivel en los riesgos de activos de información en las dos vistas siguientes:

- Conjunto de activos de información
- Privacy Splash

Conjunto de activos de información

El conjunto de activos de información es el resultado del descubrimiento y la clasificación de los datos, y es una agrupación lógica de los activos de datos de acuerdo con una taxonomía. La taxonomía se puede configurar y está asociada al contexto empresarial de la organización. Ejecute los pasos siguientes para ver la página **Conjunto de activos de información**.

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) con sus credenciales de usuario.
2. Pulse el icono de menú .
3. Pulse **Panel de control**.
4. Seleccione el programa.

5. Pulse **Panel de control**. Se mostrará la página **Conjunto de activos de información**.

Un activo de información puede tener una prioridad `Alta`, `Media` o `Baja` , en función de los criterios de puntuación predefinidos.

Para obtener más información sobre el conjunto de activos de información, consulte "Panel de control de IBM Data Risk Manager" en la página 177.

Privacy Splash

La página **Privacy Splash** es la página de destino del módulo de panel de control de IBM Data Risk Manager. La página **Privacy Splash** proporciona una visión general más amplia de la exposición al riesgo de privacidad de los activos de información a través de una serie de diagramas, mapas, gráficos, tablas, etc. Se puede visualizar y gestionar la información en varios widgets de diferentes maneras que ayudan a los líderes empresariales a analizar y abordar con rapidez los riesgos de privacidad de los datos para proteger sus organizaciones.

Siga los pasos siguientes para ver los widgets de la página **Privacy Splash** de un determinado programa.

1. Pulse **Programa** para seleccionar el programa de la lista.
2. Pulse **Imagen de pantalla de privacidad**.
3. Pulse en el icono de recarga de widget en cada uno de los widgets para renovar los datos.

Para obtener más información sobre los widgets de **Privacy Splash**, consulte "IBM Data Risk Manager Privacy Splash" en la página 173.

Configuración de esquemas de color para visualizaciones de widgets

Puede personalizar colores predeterminados de varios elementos de widget de IBM Data Risk Manager de acuerdo con sus requisitos.

Acerca de esta tarea

Los colores se pueden personalizar para los elementos siguientes.

- Widgets de bienvenida
- Widgets en Control y mandatos de seguridad
- Panel de control de IBM Data Risk Manager

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://`*`<dirección-IP-servidor-IDRM>`*`:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**.
4. Pulse el icono desplegable y seleccione **Configuración de widget**.
5. Pulse el icono desplegable situado junto a un título de widget, por ejemplo, **Widgets de bienvenida**.
6. Para modificar el esquema de color predeterminado para los elementos de widget **Distribución geográfica de los activos de información con mayor nivel de detalle del país**, ejecute los pasos siguientes.
   a) Seleccione **Residencia de datos**.
   b) Pulse el icono de editar .
   c) En la paleta de colores, seleccione un color según los requisitos.
   d) Pulse **Aceptar**.

e) Para restaurar el color predeterminado del widget, pulse el icono de restauración  .

f) ara modificar el color de otros elementos bajo **Distribución geográfica de los activos de información con mayor nivel de detalle del país**, pulse el icono desplegable  y seleccione un elemento de la lista, por ejemplo **Violaciones de política**.

g) Repita los pasos b-d.

h) Repita los mismos pasos para modificar esquemas de colores para los elementos bajo **Violaciones y vulnerabilidades de políticas que pertenecen al activo de información**.

7. Repita los mismos pasos para modificar esquemas de colores para los elementos bajo **Centro de control y mandatos de seguridad** y **Panel de control de IBM Data Risk Manager**.

IBM Data Risk Manager Privacy Splash

Se puede visualizar información de privacidad y seguridad de datos en varios widgets de la página de IBM Data Risk Manager Privacy Splash de diferentes maneras que ayudan a los líderes de negocio a analizar y abordar con rapidez los riesgos de privacidad y seguridad para proteger sus organizaciones.

La página **Privacy Splash** es la página de destino del módulo de panel de control de IBM Data Risk Manager. La página **Privacy Splash** proporciona una visión general más amplia de la exposición al riesgo de privacidad y seguridad de los activos de información a través de una serie de diagramas, mapas, gráficos, tablas, etc.

Para ver los widgets de la página **Splash** de un programa específico:

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) con sus credenciales de usuario.
2. Pulse el icono de menú  .
3. Pulse **Panel de control**.
4. Pulse **Programa** para seleccionar el programa de la lista.
5. Pulse **Imagen de pantalla de privacidad**.

Se incluyen los widgets siguientes en la página de IBM Data Risk Manager Privacy Splash:

- distribución geográfica de los activos de información
- distribución de activos de información
- principales 10 flujos de información
- vulnerabilidades e infracciones de políticas
- Clasificación
- Tendencias de vulnerabilidades trimestrales

Siga los pasos siguientes para visualizar los widgets que necesite en la página **Privacy Splash**.

1. Pulse en el icono **Widgets** 

para seleccionar los widgets que aparecen en la página.
2. Seleccione los widgets que desee visualizar en la página **Privacy Splash**.
3. Pulse **Aplicar** para guardar la configuración.

Para renovar los datos de los widgets, pulse en el icono Recargar widget  en cada uno de los widgets.

Distribución geográfica de los activos de información

El widget Distribución geográfica de los activos de información en la página **Privacy Splash** de IBM Data Risk Manager muestra ubicaciones de datos, violaciones de políticas, vulnerabilidades y ubicaciones de aplicación que están asociados a una infraestructura en un mapa global.

La sección **Orígenes de datos + Residencia** muestra información de resumen que incluye el número total de ubicaciones de origen de datos, orígenes de datos, recuentos de columnas y filas de tabla y los riesgos que están asociados a la infraestructura. La sección **Aplicaciones + Procesos de negocio** muestra información de resumen que incluye el número total de aplicaciones, procesos de negocio, flujos de datos y riesgos de datos que están asociados al inventario de aplicaciones.

Residencia de datos

Habilite el botón de conmutador **Residencia de datos** para ver la distribución de la residencia de los datos confidenciales en los países. Mueva el cursor en los círculos resaltados en el mapa global para ver información de residencia de datos en los países. En el lado izquierdo del widget, los nombres de país se visualizan junto con los números de elemento de datos.

Seleccione un país en la lista y pulse el icono de flecha para ver la distribución a nivel de estado de los datos en el mapa. Este icono para la vista detallada solo se muestra para los países soportados.

Pulse el icono de detalles para ver la lista de estados y los datos asociados. Para deseleccionar la selección de país, vuelva a pulsar el nombre de país o pulse el icono **Recargar widget**.

Violación de política

Habilite el botón de conmutador **Violación de política** para ver las violaciones de políticas que están asociadas a la infraestructura. Mueva el cursor en los círculos resaltados en el mapa global para ver detalles de violación de política en los países. En el lado izquierdo del widget, los nombres de país se muestran junto con los números de violación de política.

Seleccione un país en la lista y pulse el icono de flecha para ver la distribución a nivel de estado de los datos en el mapa. Este icono para la vista detallada solo se muestra para los países soportados.

Pulse el icono de detalles para ver la lista de estados y los datos asociados. Para deseleccionar la selección de país, vuelva a pulsar el nombre de país o pulse el icono **Recargar widget**.

Vulnerabilidades

Habilite el botón de conmutador **Vulnerabilidades** para ver la información de vulnerabilidad que está asociada a las bases de datos, puntos finales e inventarios de aplicaciones. Mueva el cursor en los círculos resaltados en el mapa global para ver información de vulnerabilidad en los países. En el lado izquierdo del widget, los nombres de los países se muestran junto con los números de vulnerabilidad.

Seleccione un país en la lista y pulse el icono de flecha para ver la distribución a nivel de estado de los datos en el mapa. Este icono para la vista detallada solo se muestra para los países soportados.

Pulse el icono de detalles para ver la lista de estados y los datos asociados. Para deseleccionar la selección de país, vuelva a pulsar el nombre de país o pulse el icono **Recargar widget**.

Residencia de la aplicación

Habilite el botón de conmutador **Residencia de la aplicación** para ver la ubicación de las aplicaciones en las geografías. En el lado izquierdo del widget, se muestra el nombre de las aplicaciones.

Cuando una aplicación está seleccionada en el panel de la izquierda, la presencia global de dicha aplicación concreta se traza en el mapa global. Puede ver los detalles siguientes para la aplicación seleccionada.

- El icono de servidor de aplicaciones muestra el recuento de servidores de aplicaciones.
- El icono Servidor de bases de datos muestra el recuento de servidores de bases de datos.
- Pulse el icono de detalles para ver la información de colocación en mapa del servidor de aplicaciones y del servidor de bases de datos y su recuento. El significado de `Sin colocación en mapa` es que la ubicación del servidor no se conoce. Puede ver las ubicaciones del servidor con localización en el mapa.
- Para deseleccionar la selección de la aplicación, vuelva a pulsar el nombre de la aplicación o pulse el icono **Recargar widget**.

- Para deseleccionar una selección de país en el mapa, pulse el icono de cruz junto al nombre del país en el panel izquierdo.

Los países soportados son Alemania, Estados Unidos de América, Canadá, Australia, Rusia, Emiratos Árabes Unidos, R.U., India, Afganistán, Francia, Sudáfrica, Italia, Países Bajos, Brasil, Japón, China, España, Argentina, México, Colombia, Chile, Paraguay, Bolivia, Uruguay, Venezuela, Mongolia, Corea del Norte, Corea del Sur, Singapur, Nueva Zelanda, Arabia Saudí, Yemen, Omán, Rumanía, Bulgaria, Grecia, Turquía, Portugal, Israel, Suiza, Austria, Bélgica, Polonia, Suecia, Noruega, Finlandia, Ucrania, Bielorrusia, Irlanda, Dinamarca, República Checa, Eslovaquia, Hungría, Croacia y Serbia.

Utilice los iconos siguientes en el widget para cambiar el tamaño del mapa y para renovar los datos.

- Pulse el icono para restablecer para restablecer el tamaño del mapa.
- Pulse el icono de acercar zoom y el icono de alejar zoom para cambiar el tamaño del mapa.
- Pulse el icono **Recargar widget** para renovar datos.

Distribución de activos de información

El widget Distribución de información de activos en la página **Privacy Splash** de IBM Data Risk Manager muestra los detalles del riesgo de privacidad y del riesgo de seguridad de activos de información que están asociados al programa seleccionado.

Para visualizar la información de riesgo, puede seleccionar atributos relacionados con la taxonomía para indicar si el activo de información tiene información joya de la corona, información que no es joya de la corona o ambas. Las entidades listadas son los atributos típicos de correlación de taxonomía en datos de contexto como, por ejemplo, Aplicación, Nivel de organización de grupo, Nivel de organización de consumo 1, Nivel de organización de consumo 2, Proceso de negocio y Activos.

Se listan todos los activos asociados al programa. El orden de clasificación se determina por clasificación, joya de la corona, categoría crítica y nivel de confidencialidad. Los riesgos de activos se visualizan para sus correspondientes activos.

Solo se visualizan los 10 principales procesos de negocio, aplicaciones y otros atributos de taxonomía. También se visualizan los riesgos de datos de nivel de aplicación y los riesgos de privacidad asociados.

Riesgo de privacidad
Puede ver inventarios de activos y su información de riesgo de privacidad correspondiente en formato tabla. El gráfico muestra las distribuciones de riesgo de privacidad de los inventarios asociados (aplicación o base de datos).

Taxonomía
Se muestran los detalles de riesgo de activo en formato tabular para las entidades seleccionadas.

Pulse en el icono **Configurar** para seleccionar las entidades. La visualización de datos se puede filtrar seleccionando las categorías de clasificación de datos necesarias. El gráfico muestra las distribuciones de riesgo en las infraestructuras.

Para renovar los datos, pulse el icono **Recargar widget** en el widget.

Los primeros 10 flujos de datos

El widget Los primeros 10 flujos de datos en la página **Privacy Splash** de IBM Data Risk Manager muestra los mapas de flujos de datos para visualizar rápidamente dónde se procesan los datos confidenciales, cómo transitan y dónde se almacenan. Los diagramas de flujo muestran las relaciones entre las entidades de negocio de una organización como, por ejemplo, los procesos de negocio, las aplicaciones y la infraestructura.

Los diagramas de flujo de datos se pueden visualizar en función de los orígenes de datos, los procesos de negocio y las aplicaciones. Para ver más detalles, pase el cursor sobre un elemento del diagrama.

Origen de datos
Se muestra el diagrama de flujo de datos del origen de datos seleccionado para ver la información de riesgo de privacidad y de riesgo de datos.

Aplicación
Se muestra el diagrama de flujo de datos de la aplicación seleccionada para ver la información de riesgo de privacidad y de riesgo de datos.

Proceso
Se muestra el diagrama de flujo de datos del proceso seleccionado para ver la información de riesgo de privacidad y de riesgo de datos.

Para renovar los datos, pulse el icono **Recargar widget** en el widget.

Violaciones de políticas y vulnerabilidades

El widget Violaciones de políticas y vulnerabilidades en la página **Privacy Splash** de IBM Data Risk Manager muestra el desglose de las violaciones de políticas y las vulnerabilidades en los activos de información.

El gráfico muestra los 10 primeros activos de información. También se pueden ver los iconos que indican los detalles de nivel de riesgo y de joya de la corona de los activos de información. El orden de clasificación se determina por clasificación, joya de la corona, categoría crítica y nivel de confidencialidad.

Para renovar los datos, pulse el icono **Recargar widget** en el widget.

Clasificación

El widget Clasificación en la página **Privacy Splash** de IBM Data Risk Manager le proporciona una vista rápida sobre la clasificación de seguridad de activos de información. Los detalles de confidencialidad de los datos se presentan en forma de diagrama circular y formato de vista de lista que ayuda a comunicar la información de forma clara y eficaz.

Para ver la información de confidencialidad en formato de gráfico circular, pulse en el icono de gráfico circular . La vista de diagrama es la predeterminada.

Para ver la información de confidencialidad en formato de vista de lista, pulse en el icono de vista de lista .

La información de clasificación de datos se basa en los siguientes criterios. Seleccione las opciones **Todo**, **Con joya de la corona** o **Sin joya de la corona** para que la información de clasificación se ajuste a sus necesidades.

Categorías
Pulse en **Categorías** para ver la información de clasificación de datos en función de diversas categorías. Pase el cursor sobre las cuñas del gráfico circular para ver el valor porcentual de las distintas categorías. Pulse en una sección para visualizar la información detallada.

Activos etiquetados
Pulse **Activos etiquetados** para ver la información de clasificación de datos en función de un nombre de etiqueta que identifica un grupo de activos de información relacionados. Pase el cursor sobre las cuñas del gráfico circular para ver el valor porcentual de los distintos activos etiquetados. Pulse en una sección para visualizar la información detallada.

Conformidad
Pulse **Conformidad** para ver la información de clasificación de datos en función de las obligaciones normativas asociadas al activo como, por ejemplo, HIPAA, SOX o PCI. Pase el cursor sobre las cuñas del gráfico circular para ver el valor porcentual de cada tipo de información de conformidad. Pulse en una sección para visualizar la información detallada.

Para renovar los datos, pulse el icono **Recargar widget** en el widget.

Tendencias de vulnerabilidades trimestrales

El widget Tendencias de vulnerabilidades trimestrales en la página **Privacy Splash** de IBM Data Risk Manager muestra los detalles de las tendencias de vulnerabilidades trimestrales para las exploraciones que se ejecutan entre distintos puntos finales de bases de datos y plataformas de aplicación. Mueva el botón de conmutación para ver las tendencias de exploraciones de vulnerabilidad pasadas y fallidas.

Las plataformas asociadas a los activos de información se visualizan debajo del gráfico. Pulse en una plataforma para ver información detallada relativa a las vulnerabilidades en función de los detalles de gravedad como, por ejemplo, Crítico, Mayor, Menor o Precaución.

Para renovar los datos, pulse el icono **Recargar widget**  en el widget.

Panel de control de IBM Data Risk Manager

El panel de control de IBM Data Risk Manager es un panel interactivo que habilita el gobierno de información proporcionando visualización y gestión en una única consola unificada que representa los riesgos potenciales para los activos de empresa confidenciales.

Funciones del panel de control de IBM Data Risk Manager

- Proporciona una visualización interactiva de la cartera de activos de información, la clasificación de datos y los requisitos de seguridad.
- Permite la aplicación de controles de seguridad proactivos y la mitigación de riesgos al proporcionar visibilidad de riesgos potenciales, exposiciones y vulnerabilidades.
- Combina activos de información, procesos y metadatos de controles para representar la seguridad de datos y la posición de control.
- Habilita el control de información que permite a los líderes de negocio visualizar los riesgos en los activos confidenciales en todas las funciones de negocio y ayuda a comprender la posible repercusión en la organización.
- Proporciona supervisión de conformidad a través de notificaciones en tiempo real y elementos de acción en alineación con las políticas y requisitos de seguridad de datos.

Conjunto de activos de información

El widget **Conjunto de activos de información** en el panel de control muestra la clasificación de todos los activos de información asociados a un programa basándose en un modelo de taxonomía seleccionado por el usuario. El activo de información es el concepto central de IBM Data Risk Manager y se puede definir como una agregación o una agrupación de elementos de datos relacionados que juntos representan un activo de negocio.

El conjunto de activos proporciona las funciones siguientes.

- Visualizar todos los activos de información asociados a un programa.
- Visualizar los activos de información de una manera que represente el sentido empresarial.

La vista predeterminada muestra activos de información que están asociados al programa seleccionado. El eje X muestra clasificaciones de información. El eje Y muestra el programa y subprogramas. Puede modificar dinámicamente la representación de taxonomía. Esta taxonomía se puede configurar para el contexto empresarial de la organización. Para cambiar los atributos de los ejes X y Y para un programa, ejecute los pasos siguientes.

1. Pulse el programa en el eje X.
2. Pulse los botones de flecha  junto a las etiquetas para seleccionar los atributos.

Cuando se selecciona un activo de información en el widget **Conjunto de activos de información**, todos los metadatos que están asociados al activo de información seleccionado se muestran en los widgets circundantes como, por ejemplo, **Infraestructuras**, **Partes interesadas**, **Procesos** y **Aplicaciones**.

Los distintos microiconos y números en un activo de información proporcionan los detalles de metadatos técnicos y de negocio siguientes que están asociados al activo de información seleccionado.

Icono	Descripción
	El numérico junto al icono indica el número de violaciones de políticas. Pulse el icono para ver incidencias en la ventana Registros de activos que se registran (según la gravedad) en relación con el activo de información seleccionado. En la ventana **Registros de activos**, pulse los elementos para ver los detalles de la alerta.
	El numérico junto al icono representa el número de elementos de datos granulares que están asociados al activo de información.
	Pulse el icono para ver la valoración de Confidencialidad-Integridad-Disponibilidad (CIA) para el activo de información.
	Indica que el activo de información tiene información del tipo joya de la corona.
	Representa la puntuación de riesgo para el activo de información como, por ejemplo, alto (rojo), medio (ámbar), bajo (verde) o sin riesgo (gris). Pulse el icono para ver los factores que se tienen en cuenta para calcular la puntuación de riesgo.

Puede personalizar los colores predeterminados de la tarjeta de activos de información y de los elementos de metadatos asociados. Para ver los pasos sobre cómo personalizar los colores, consulte "Configuración de esquemas de color para visualizaciones de widgets" en la página 172.

Utilice los iconos siguientes en el widget **Conjunto de activos de información** para ejecutar distintas tareas.

- Habilite el botón de conmutador **Mostrar todos los datos del nivel** para ver los activos de los programas de nivel inferior también para un programa padre seleccionado.
- Habilite el botón de conmutador **Mostrar etiquetas de activo** para ver información para las etiquetas asignadas. Pulse el icono **Filtrar activos basados en etiqueta**  para mostrar los activos basados en la etiqueta seleccionada.
- Pulse el icono **Filtrar activos**  para ver activos de información basados en atributos como, por ejemplo, `Joyas de la corona`, `Clasificación de información` o `Conformidad`.
- Pulse el icono de renovación  para renovar los datos de widget.
- Pulse el icono para expandir  para expandir el área del widget.
- Pulse el icono de flecha  en el activo de información para ver más detalles de elementos de datos en la ventana **Detalles de activo**.

Desglose de activo de información

En el widget **Conjunto de activos de información**, pulse el icono de flecha  en el activo para mostrar la ventana emergente **Detalles de activo** y ver los detalles del activo seleccionado.

Visión general

Proporciona información granular acerca de las tablas y columnas en las que reside el activo de información y la lista de atributos asignados para las aplicaciones asociadas.

Nota: Los activos no estructurados no están asociados a ninguna aplicación. Por lo tanto, los atributos de taxonomía no son aplicables a los activos no estructurados.

Infraestructura

Puede ver la información siguiente.

- Lista de orígenes de datos con detalles como, por ejemplo, el porcentaje de contribución de datos, la dirección IP, el número de puerto, la ubicación del origen de datos y partes interesadas.
- Violaciones de políticas que se registran en relación con los nodos de infraestructura bajo **Violaciones de políticas**.
- Vulnerabilidades que se registran con respecto a los nodos de infraestructura bajo **Vulnerabilidades**.
- Riesgos que están asociados a los nodos de infraestructura bajo **Riesgos**.

Puede ver las violaciones de política, los detalles de vulnerabilidad y la información de riesgos en función de la opción de filtro seleccionada como, por ejemplo, los orígenes o la gravedad. Cuando se selecciona una violación de política, una vulnerabilidad o un elemento de riesgo, se puede ver la información siguiente.

- Más detalles sobre el elemento seleccionado bajo **Detalles**.
- Acciones de reparación que están definidas para el elemento seleccionado bajo **Elementos de acción**.
- Configuración de correo bajo **Correo**.

Infraestructuras

El widget Infraestructuras muestras las infraestructuras (plataformas) que están asociadas al activo de información. Los elementos de datos pueden incluir repositorios estructurados y no estructurados. Pulse el icono desplegable en una infraestructura para ver los repositorios de datos y sus atributos. Los atributos siguientes se muestran para el repositorio seleccionado.

- Nombre de repositorio de datos, dirección IP, puerto y ubicación geográfica.
- Número de alertas que se registran con respecto al nodo de infraestructura.
- Número de vulnerabilidades que se registran con respecto al nodo de infraestructura.
- Porcentaje de contribución de datos.
- El icono de estado de cifrado indica si el origen de datos está cifrado.
- El icono de estado de supervisión indica si el origen de datos está supervisado.
- El icono de estado de exploración de vulnerabilidades indica si la exploración de evaluación de vulnerabilidades se ejecuta en el origen de datos.
- El icono de riesgos de datos indica si la puntuación de riesgo es alta (roja), media (ámbar) o baja (verde) para esta infraestructura específica. Pulse el icono para ver los detalles de distintos vectores de riesgo junto con los factores asociados que se tienen en cuenta para el cálculo de riesgo. También puede ver el nivel de impacto que se calcula basándose en los atributos de taxonomía del activo de información y la puntuación de riesgo de la infraestructura.
- El icono de riesgos de privacidad indica si la puntuación de riesgo de privacidad es alta (rojo), media (ámbar) o baja (verde) para esta infraestructura específica.
- Pulse el icono de correlaciones para ver la relación de esta infraestructura con otras entidades como, por ejemplo, procesos de negocio y aplicaciones que están asociados al activo de información.
- Pulse el icono de descarga para descargar los archivos CSV que contienen atributos específicos de la infraestructura.
- Pulse el icono de correlaciones de datos para ver la ventana emergente, que muestra los atributos específicos de la infraestructura que están configurados y agrupados basándose en un contexto.

Partes interesadas

El widget `Parte interesada` muestra las partes interesadas asociadas al activo de información seleccionado. El widget se puede configurar para representar una infraestructura de partes interesadas que se puede personalizar para una organización. Pulse en cualquiera de las secciones circulares para ver a la parte interesada correspondiente en la organización.

Procesos

El widget `Procesos` muestra los procesos de negocio que están asociados al activo de información seleccionado. Estos son los procesos de negocio en una organización que dependen del activo de información para realizar transacciones de negocio. Los atributos que están asociados a procesos de negocio se pueden personalizar para la estructura de la organización.

En un proceso seleccionado, pulse el icono `***` para ver la ventana emergente, que muestra los atributos específicos del proceso de negocio que están configurados y agrupados basándose en un contexto. Para descargar el archivo PDF con atributos específicos de proceso, pulse el icono Descargar  .

Aplicaciones

El widget Aplicación muestra las aplicaciones que están asociadas al activo de información seleccionado. Estas son las aplicaciones que producen, consumen o utilizan el activo de información. Los atributos que están asociados a las aplicaciones se pueden personalizar para la estructura de organización. Los recuentos de vulnerabilidades y de alertas se muestran si el servidor de aplicaciones alojado contiene vulnerabilidades asociadas y violaciones de políticas. Los atributos siguientes se muestran para la aplicación seleccionada.

- El número de alertas que se registran en relación con servidor de aplicaciones alojado. Pulse el número para ver más detalles.
- El número de vulnerabilidades de aplicación que se registran en relación con el servidor de aplicaciones alojado.
- El icono de riesgos de datos indica si la puntuación del riesgo de datos es alta, media o baja para este servidor de aplicaciones específico.
- El icono de riesgos de privacidad indica si la puntuación del riesgo de privacidad es alta, media o baja para este servidor de aplicaciones específico.
- Pulse en el icono de correlaciones de datos  para ver la ventana emergente contextual, que muestra atributos específicos de aplicación configurados y agrupados en función de un contexto.
- Pulse el icono de descarga  para descargar el archivo PDF con los atributos específicos de la aplicación.

Informe de riesgos, exposiciones y vulnerabilidades (REV)

IBM Data Risk Manager se puede utilizar para identificar riesgos potenciales en activos de información confidencial sobre la empresa. Basándose en la disponibilidad de dicha información, IBM Data Risk Manager superpone los vectores de riesgo que se componen de incidencias de supervisión de actividad, exposiciones y vulnerabilidades, y una actividad maliciosa potencial en varios niveles. Los vectores de riesgo brindan visibilidad a las partes interesadas adecuadas y les permiten iniciar medidas correctivas. Por ejemplo, los vectores de riesgo superpuestos sobre los activos de información proporcionan un aviso de las partes interesadas del negocio sobre un riesgo asociado al activo de empresa, mientras que dicha información superpuesta sobre los repositorios de datos es indicativa de una parte interesada técnica.

Creador de infraestructuras

Puede utilizar el componente Creador de infraestructuras de IBM Data Risk Manager para crear y gestionar infraestructuras, plantillas de cuestionarios, cuestionarios y registros necesarios para realizar las evaluaciones.

El creador de infraestructura de IBM Data Risk Manager proporciona las funciones siguientes.

Creador de infraestructuras
Crear y gestionar infraestructuras de evaluaciones, temas, subtemas y factores. Para obtener más información sobre el creador de infraestructura, consulte “Creador de infraestructuras de IBM Data Risk Manager” en la página 181.

Creador de cuestionario
Crear y gestionar plantillas de cuestionarios y cuestionarios. Para obtener más información sobre el creador de cuestionario, consulte “Creador de cuestionario” en la página 183.

Definiciones de registro
Gestionar registros y crear elementos de registro. Para obtener más información sobre las definiciones de registro, consulte “Definiciones de registro” en la página 187.

Creador de infraestructuras de IBM Data Risk Manager

Puede utilizar el componente Creador de infraestructuras de IBM Data Risk Manager para crear y gestionar las infraestructuras necesarias para realizar las evaluaciones de riesgo. Una infraestructura es un requisito normativo o de cumplimiento de normativas con el que se mide la conformidad de los datos en las implementaciones de control de una organización.

Un creador de infraestructuras consta de los objetos siguientes.

Tema
El primer nivel de una jerarquía de infraestructuras con una o varias subsecciones, cada una de las cuales cubre un objeto de control. Un tema es una agregación de subtemas.

Subtema
Incluye especificaciones de requisitos funcionales para una infraestructura con controles asociados. Un subtema es una agregación de factores.

Factor
El nivel más bajo de una jerarquía de infraestructuras con controles asociados.

Infraestructuras de evaluación

Puede crear los siguientes tipos de infraestructuras de evaluación mediante el Creador de infraestructuras de IBM Data Risk Manager.

PRA
Crea infraestructuras para evaluar controles que se ajusten a los requisitos de la normativa GDPR (General Data Protection Regulation). Cuando crea una evaluación, si selecciona la infraestructura GDPR, de forma predeterminada, se crean cinco evaluaciones.

No PRA
Crea infraestructuras para evaluar controles que se ajusten a requisitos que no son de GDPR, por ejemplo, la infraestructura ISO. Para crear una evaluación, debe utilizar temas, subtemas y factores creados utilizando el Creador de infraestructuras.

Crear una infraestructura

Puede utilizar el Creador de infraestructuras de IBM Data Risk Manager para crear y gestionar las infraestructuras necesarias para realizar las evaluaciones de datos.

Acerca de esta tarea

Un creador de infraestructuras consta de los objetos siguientes.

Tema
El primer nivel de una jerarquía de infraestructuras con una o varias subsecciones, cada una de las cuales cubre un objeto de control. Un tema es una agregación de subtemas.

Subtema
Incluye especificaciones de requisitos funcionales para una infraestructura con controles asociados. Un subtema es una agregación de factores.

Factor
El nivel más bajo de una jerarquía de infraestructura con un conjunto de preguntas sobre una implementación de control.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Creador de infraestructuras** > **Creador de infraestructuras**.
4. En la sección **Creador de infraestructuras**, establezca las opciones siguientes y pulse **Crear**.

Opción	Descripción
Nombre	El nombre de la infraestructura.
Nombre de visualización	El nombre de visualización de la infraestructura.
Descripción	La descripción de la infraestructura.
Controles	Selección de controles de seguridad de datos para asociar con la infraestructura. Puede definir más controles en **Definiciones de registro** para un registro predefinido, por ejemplo, `DictControl`.
Asignar	Selección de una plantilla de cuestionario para asociar con la infraestructura. Las plantillas que se crean en **Creador de cuestionario** se muestran en la lista **Asignar**.
Tipo de entorno	Selección de tipo de infraestructura de evaluación, por ejemplo, **NON PRA** o **PRA**. Seleccione PRA para crear la infraestructura GDPR. Seleccione NON PRA para crear una infraestructura no GDPR.

Qué hacer a continuación
Cree temas, subtemas y factores para la infraestructura que ha creado. Para obtener más información, consulte “Crear un tema, subtema y factor para una infraestructura” en la página 182

Crear un tema, subtema y factor para una infraestructura
Asocie un tema, subtema y factor para la infraestructura de evaluación que ha creado. Una infraestructura es un requisito normativo o de cumplimiento de normativas con el que se mide la conformidad de los datos en las implementaciones de control de una organización.

Antes de empezar
Asegúrese de que las infraestructuras se han creado y están disponibles para su uso.

Acerca de esta tarea

Un creador de infraestructuras consta de los objetos siguientes.

Tema
El primer nivel de una jerarquía de infraestructuras con una o varias subsecciones, cada una de las cuales cubre un objeto de control. Un tema es una agregación de subtemas.

Subtema
Incluye especificaciones de requisitos funcionales para una infraestructura con controles asociados. Un subtema es una agregación de factores.

Factor
El nivel más bajo de una jerarquía de infraestructura con un conjunto de preguntas sobre una implementación de control.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Creador de infraestructuras** > **Creador de infraestructuras**.
4. En **Entornos creados**, pulse **Temas** en la infraestructura para la que desea crear un tema.
5. En la sección **Creador de infraestructuras**, establezca las opciones siguientes.

Opción	Descripción
Nombre	El nombre del tema.
Nombre de visualización	El nombre de visualización del tema.
Descripción	Descripción del tema.
Controles	Selección de controles de seguridad de datos para asociar con el tema. Puede definir más controles en **Definiciones de registro** para un registro predefinido, por ejemplo, `DictControl`.

6. Pulse **Crear**.
7. Cree un subtema.
   a) En **Temas creados**, pulse **Subtemas** en el tema para el que desea crear un subtema.
   b) Especifique los detalles necesarios en los campos correspondientes que cumplen sus necesidades de negocio.
   c) Pulse **Crear**.
8. Cree un factor.
   a) En **Subtemas creados**, pulse **Factores** en el subtema para el que desea crear un factor.
   b) Especifique los detalles necesarios en los campos correspondientes que cumplen sus necesidades de negocio.
   c) Pulse **Crear**.

Creador de cuestionario

Utilice la función Creador de cuestionarios de IBM Data Risk Manager para crear y gestionar plantillas y cuestionarios necesarios para realizar evaluaciones.

Cuestionarios

Los cuestionarios se crean para recopilar respuestas de usuario para evaluar la disposición o comprender la madurez de los controles. Utilice los cuestionarios de evaluación de IBM Data Risk Manager para definir y asociar los flujos de contexto necesarios para la delegación y la recopilación de pruebas, y para capturar atributos de contexto como por ejemplo la prioridad, la significancia, la relevancia y la aplicabilidad. Las

preguntas se pueden asociar con varias plantillas y se pueden personalizar para utilizarlas en varias infraestructuras de evaluación. En función del tipo de respuestas previstas para una pregunta, se puede crear y configurar un tipo de pregunta adecuada. Para ver los pasos sobre cómo crear un cuestionario, consulte “Crear una pregunta” en la página 185.

Importar datos de cuestionario

También puede importar un cuestionario predefinido para utilizarlo en la evaluación. Los datos para un cuestionario de evaluación, un tipo de respuesta y un registro se definen en un archivo de valores separados por comas (CSV), que puede importar en IBM Data Risk Manager. Para obtener más información sobre cómo importar los datos de cuestionario, consulte “Importación del cuestionario de evaluación, del tipo de respuesta y del registro como archivo CSV” en la página 188.

Plantillas de cuestionario

Una plantilla de cuestionario es un instrumento de evaluación que consta de una serie de preguntas y otras instrucciones para recopilar respuestas de personas para evaluar la madurez de un control. Puede reutilizar las plantillas en varias infraestructuras de evaluación. Para ver los pasos sobre cómo crear una plantilla de cuestionario, consulte “Creación de una plantilla de cuestionario” en la página 184.

Árbol de decisiones

Las respuestas a algunas preguntas llevan a preguntas adicionales. Puede expresar esta relación creando una relación condicional entre preguntas. En una relación condicional, hay una pregunta padre y una respuesta hijo. De forma predeterminada, la pregunta hijo no se visualiza. La pregunta hijo se visualiza solo cuando se proporciona una respuesta habilitadora a la pregunta padre. Mediante el árbol de decisiones, puede ver e identificar rápidamente las relaciones entre las preguntas.

El árbol de decisiones es una estructura jerárquica que consta de nodos y bordes dirigidos. Un árbol de decisiones normalmente se inicia con un solo nodo (pregunta padre), que se ramifica (preguntas hijo) en los posibles resultados. Cada uno de estos resultados puede llevar a nodos adicionales, que se ramifican en otras posibilidades. Mediante un árbol de decisiones, puede explicar fácilmente las decisiones, identificar posibles sucesos que podrían producirse y ver los posibles resultados.

Creación de una plantilla de cuestionario

Puede utilizar el Creador de cuestionario de IBM Data Risk Manager para crear una plantilla de cuestionario. Una plantilla puede estar asociada a una serie de preguntas y otras instrucciones pensadas para recopilar respuestas de las personas. Puede reutilizar una plantilla en varias infraestructuras de evaluación.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Creador de infraestructuras** > **Creador de cuestionario**.
4. Para crear una plantilla, pulse **Nueva plantilla**.
5. En la sección **Crear plantilla**, establezca las opciones siguientes y pulse **Crear**.

Opción	Descripción
Nombre	El nombre de la plantilla.
Categoría	La categoría de la plantilla, por ejemplo, `Evaluación`.
Descripción	La descripción de la plantilla.

Opción	Descripción
Modelo de puntuación	El modelo de puntuación que se ha de usar para el cálculo de puntuación de la evaluación, por ejemplo, `Promedio ponderado` o `Método condicional`.
Metodología de cálculo	Puede especificar un método de cálculo de la puntuación únicamente cuando selecciona `Método condicional` en la lista **Modelo de puntuación**.
Plantilla de puntuación	Puede especificar una plantilla de puntuación con la escala de puntuación predefinida. Si selecciona `Método condicional` en la lista **Modelo de puntuación**, puede establecer las condiciones para la plantilla de puntuación seleccionada.

Crear una pregunta

Puede utilizar un creador de cuestionarios de IBM Data Risk Manager para crear preguntas para la evaluación y asociarlas a varias plantillas de cuestionarios.

Acerca de esta tarea

También puede definir datos para cuestionario de evaluación en un archivo de valores separados por comas (CSV), que puede importar a IBM Data Risk Manager. Para ver los pasos sobre cómo importar cuestionarios, consulte "Importación del cuestionario de evaluación, del tipo de respuesta y del registro como archivo CSV" en la página 188.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Creador de infraestructuras** > **Creador de cuestionario**.
4. Para crear una pregunta, pulse **Nueva pregunta**.
5. En la sección **Crear pregunta**, establezca las opciones siguientes y pulse **Guardar**.

Opción	Descripción
Preguntas	El texto de la pregunta.
Descripción	La descripción de la pregunta.
Prioridad de pregunta	Puede dar prioridad a la pregunta en la infraestructura definida, especificando la prioridad como alta, media, informativa o baja. Se puede añadir un elemento a la lista **Prioridad de pregunta** creando un elemento de registro en el registro de **Prioridad de preguntas** en **Modelador de contextos de negocio** > **Creador de infraestructuras** > **Registrar definiciones**. Para ver los pasos de creación de un elemento de registro, consulte "Crear un elemento y subelemento para el registro" en la página 187.
Grupo de preguntas	Puede asociar la pregunta a un grupo predefinido. Durante la evaluación, puede ver las preguntas con las respuestas en función del grupo asignado al crear la pregunta. Se puede añadir un grupo a la lista **Grupo de preguntas** creando un elemento de registro en el registro de **Agrupador de preguntas** en **Modelador de contextos de negocio** > **Creador de infraestructuras** > **Registrar definiciones**. Para ver los pasos de creación de un elemento de

Opción	Descripción
	registro, consulte “Crear un elemento y subelemento para el registro” en la página 187.
Tipo de respuesta	El tipo de visualización de las opciones de preguntas, tales como lista de varias selecciones, botón de selección y tipo de escala.
Capítulo	Número de capítulo de la infraestructura.
Sección	Número de sección de la infraestructura.
Artículo	Número de artículo de la infraestructura.
Artículo de referencia	Número de artículo de referencia de la infraestructura.
Dependencia de pregunta	Las respuestas a algunas preguntas llevan a preguntas adicionales. Se puede expresar esta relación creando una relación condicional entre preguntas y mostrándolas en forma de un árbol de decisiones. a. Pulse el icono Añadir . b. Seleccione **And** u **OR** según los requisitos. c. Seleccione preguntas dependientes de la lista. d. Establezca las condiciones para los atributos de las preguntas seleccionadas. e. Pulse **Guardar condiciones**.
Opciones de respuesta	Defina las opciones de respuesta para la pregunta. a. Pulse el icono Añadir . b. Especifique el texto de la respuesta en **Texto de respuesta**. c. Añada una descripción de la respuesta en **Descripción**. d. Asigne un valor de puntuación. 1) Especifique una puntuación de la respuesta en el rango de 0 a 5 en **Puntuación de respuesta**. Para proporcionar respuesta a una pregunta de tipo **Escala**, especifique valores en los campos **Valor mínimo**, **Valor máximo** y **Descripciones de valor de escala**. 2) Seleccione el tipo de contexto en **Tipo de contexto**. 3) Pulse **Añadir** para definir observaciones especificando una prioridad. La especificación de la puntuación de respuesta no es necesaria cuando la puntuación de cálculo se genera seleccionando **Puntuación de cálculo**. e. Para generar puntuación de cálculo, ejecute los pasos siguientes. 1) Seleccione **Puntuación de cálculo**. 2) Seleccione **Estándar** para asignar puntuación según las otras respuestas que seleccione. 3) Seleccione una opción en la lista **Fórmula de cálculo**. 4) Seleccione las respuestas en la lista **Respuesta a tener en cuenta**. 5) Seleccione **Condicional** para asignar puntuación según las condiciones que defina.

Opción	Descripción
	6) Pulse el icono Añadir  para añadir una condición. 7) Especifique valores en los campos **Método**, **Operador**, **Valor** y **Valor de puntuación**. f. Si desea que la puntuación de respuesta se considere para la evaluación, seleccione **Considerar para puntuación**. g. Especifique las palabras clave de respuesta en **Palabras clave de respuesta**. h. Pulse **Guardar respuesta**.
Registro	El registro asociado a la pregunta.
Ámbito	Se muestran los elementos para que los seleccione, en función del registro seleccionado en **Registro**.

6. La pregunta que ha creado se lista en la sección **Todas las preguntas**. Puede asociar plantillas a la pregunta que ha creado.
   a) Seleccione las preguntas en la lista.
   b) Pulse **Asignar**.
   c) Seleccione plantillas en la lista **Asignar plantillas**.
   d) Pulse **Confirmar**.
   e) Para modificar la información de selección de plantilla, pulse **Plantilla**.
7. Pulse **Árbol de decisiones** en una pregunta para ver la relación condicional entre preguntas en formato de árbol de decisiones.
8. El icono **Pregunta dependiente**  en una pregunta representa la relación condicional con otras preguntas.
9. Pulse **Filtro** para visualizar las preguntas asociadas con el **Registro** y **Ámbito** que seleccione.

Definiciones de registro

Puede utilizar las definiciones de registro de IBM Data Risk Manager para crear elementos y subelementos para los registros predefinidos. Estos elementos y subelementos se utilizan para la creación de infraestructuras de evaluación.

Crear un elemento y subelemento para el registro

Puede utilizar las definiciones de registro de IBM Data Risk Manager para crear elementos y subelementos para un registro predefinido.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Vaya a **Modelador de contexto empresarial** > **Creador de infraestructuras** > **Definiciones de registro**.
4. Seleccione un recurso en la lista **Registros**.
5. Para crear una elemento, pulse **Nuevo elemento de registro**.
6. Establezca las opciones siguientes y pulse **Guardar**.

Opción	Descripción
Nombre	El nombre del elemento.
Nombre de visualización	El nombre de visualización del elemento.
Descripción	La descripción del elemento.

Se muestra el elemento que ha creado en la lista **Elementos**.

7. Para añadir un subelemento, seleccione un elemento en la lista.
   a) Pulse **Añadir**.
   b) Especifique la información del subelemento, tal como el nombre, el nombre de visualización y la descripción.
   c) Pulse **Guardar**.
8. Para añadir una propiedad al elemento, ejecute los pasos siguientes.
   a) Pulse **Propiedad**.
   b) Pulse el icono Añadir .
   c) Especifique el nombre en **Nombre de propiedad**.
   d) Especifique el valor en **Valor de propiedad**.
   e) Pulse **Guardar**.
   f) Pulse el icono de recuadro de color **Valor de propiedad** para elegir el color de propiedad que se mostrará en el panel de control de IBM Data Risk Manager.
9. Para asignar elementos para un elemento seleccionado, ejecute los pasos siguientes.
   a) Pulse el icono **Asignar** .
   b) Seleccione elementos en la lista.
   c) Pulse **Asignar**.

Importación del cuestionario de evaluación, del tipo de respuesta y del registro como archivo CSV

Puede definir los datos para el cuestionario de evaluación, el tipo de respuesta y el registro en un archivo de valores separados por comas (CSV), que puede importar a IBM Data Risk Manager.

Antes de empezar

Asegúrese de que los datos de contexto empresarial estén disponibles para importarlos.

Puede descargar las plantillas de ejemplo en: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**.
4. Habilite el botón de conmutación **Datos de catálogo**.
5. Pulse la pestaña **Evaluación**.
6. Cargue el archivo CSV para el tipo de respuesta.
   a) En **Tipo de respuesta**, pulse **Examinar** para localizar y seleccionar el archivo.

b) Pulse **Cargar**.

Los datos se visualizan para su verificación.

7. Cargue el archivo CSV para el cuestionario de evaluación.
   a) En **Cuestionario**, pulse **Examinar** para localizar y seleccionar el archivo.
   b) Pulse **Cargar**.

   Los datos se visualizan para su verificación.
8. Cargue el archivo CSV para los registros.
   a) En **Registro**, pulse **Examinar** para localizar y seleccionar el archivo.
   b) Pulse **Cargar**.

   Los datos se visualizan para su verificación.
9. Pulse **Importar**.

Evaluaciones

Puede utilizar el componente Evaluación de IBM Data Risk Manager para crear evaluaciones. Una evaluación es un conjunto de preguntas personalizado, o estándar del sector, que genera un resultado. Las evaluaciones son un medio de recopilar información de los usuarios empresariales en la organización. Los resultados de la evaluación se pueden utilizar para determinar valoraciones de activos, análisis de deficiencias, puntuación de riesgos y para la planificación de reparaciones.

La característica Evaluación de IBM Data Risk Manager proporciona una infraestructura de seguridad de datos para evaluar los controles en línea con los requisitos normativos. La evaluación se basa en la utilización de cuestionarios y una puntuación consolidada.

- Plataforma para crear una evaluación personalizada para las regulaciones e infraestructuras de seguridad, gobierno y gestión seleccionadas, como por ejemplo ISO 27002.
- Puede evaluar y comprender la disposición para normativas de conformidad, como por ejemplo la normativa GDPR (General Data Protection Regulation), políticas corporativas, procedimientos y directrices.
- Capture u obtenga información con plantillas personalizadas para recopilar respuestas, pruebas, notas y reasignaciones.
- Capture información de entidades de datos de contexto durante la valoración de evaluación para el cálculo de puntuación de riesgo.
- Puntuación e informes interactivos para la evaluación de disposición y madurez.
- Integración con el Centro de acción de IBM Data Risk Manager para crear y gestionar elementos de acción de reparación para resolver deficiencias de la evaluación.

El componente **Modelador de contexto empresarial** > **Creador de infraestructuras** de IBM Data Risk Manager se utiliza para crear la estructura de evaluación y la definición del flujo de trabajo, tales como el modelado de la infraestructura y el desarrollo del cuestionario. Para obtener más información sobre el Creador de infraestructuras, consulte “Creador de infraestructuras” en la página 181.

Ámbito de evaluación

Durante la creación del programa de evaluación para infraestructuras no basadas en PRA, se puede definir el ámbito de la evaluación en términos de entidades de negocio o dominios como, por ejemplo, procesos de negocio, aplicaciones y activos. El uso de ámbitos en la evaluación garantiza la recopilación de los datos necesarios de un forma eficaz y eficiente para evaluar riesgos.

Modelado de riesgos

El riesgo se calcula en función de diversos factores como, por ejemplo, la importancia de una determinada pregunta, la respuesta asociada, los activos asignados y su importancia (clasificación),

amenazas y eventos correlacionados, y otros criterios definidos como parte de la personalización del cuestionario.

Las respuestas al cuestionario de evaluación se tienen en cuenta a la hora de determinar la puntuación de riesgo global y las acciones correctivas. Estos criterios pueden incluir factores de sensibilidad como, por ejemplo, Confidencialidad, Disponibilidad e Integridad (CAI en sus siglas en inglés) y impacto empresarial como, por ejemplo, el coste asociado, la clasificación de activos o la importancia. El riesgo residual se calcula automáticamente y la puntuación se ajusta en función de la terminación de los elementos de acción definidos para abordar las lagunas o los hallazgos, si los hay.

Evaluación para GDPR

IBM Data Risk Manager se ajusta a la normativa GDPR (General Data Protection Regulation) adoptada por los países de la UE y EEE. Establece una protección armonizada y reforzada para los datos personales de los usuarios. IBM Data Risk Manager soporta la conformidad de los datos proporcionando la evaluación y el cuestionario. Con la implementación de la evaluación de IBM Data Risk Manager, se manejan los requisitos siguientes.

- Visibilidad de la posición de riesgo de seguridad que está asociada a los datos confidenciales.
- Mayor definición de los datos personales, incluida la información de ubicación y los identificadores en línea.
- Nuevas obligaciones para los procesadores con impacto contractual, operativo y técnico.
- Ayuda a habilitar la seguridad analizando las diversas lagunas del entorno de seguridad de datos actual.
- Ayuda a determinar los controles y da prioridad a las tareas destinadas a resolver los espacios vacíos y desarrollar un plan de acción.

Gestión de resultados de evaluación

Basándose en los resultados de la evaluación no PRA, se deben implementar las acciones apropiadas para abordar y mitigar los riesgos identificados. Puede utilizar el módulo Gestión del resultado de evaluación de IBM Data Risk Manager para ver y gestionar los riesgos. Para obtener más información sobre la gestión por resultados, consulte “Gestión de resultados de evaluación” en la página 201.

Rol de persona para evaluaciones

Rol de persona para evaluación	Funciones	Descripción

Administrador	Definición y gestión de los programas	Establecer el ámbito y los límites de la evaluación como un programa basado en diferentes factores, tales como unidades empresariales, plataformas, usuarios y roles.
	Creación y configuración de infraestructuras	Definir y desarrollar infraestructuras personalizadas para evaluaciones con diferentes categorías y para asociar preguntas sobre diferentes factores, etiquetas y plantillas.
	Modelado de evaluaciones • Definiciones de preguntas • Creación de plantillas • Definiciones de programas de evaluación	Definir preguntas, opciones de respuesta para las respuestas asociadas, añadir a plantillas y asignar a temas de infraestructura, subtemas y factores.
	Suministro de usuarios y acceso	Definir usuarios y roles en diferentes recursos para acceder a IBM Data Risk Manager y proporcionar acceso a programas y evaluaciones.
Asesor **Usuario de evaluación C3** (rol de usuario de IBM Data Risk Manager)	Definiciones de evaluaciones y creación de entrevistas	Definir evaluaciones basadas en la infraestructura y crear entrevistas para las evaluaciones respectivas para calcular las puntuaciones de riesgo basadas en el análisis de deficiencias y las averiguaciones.
	Captura de información y puntuación de riesgos	Las respuestas al cuestionario se capturan mediante las opciones disponibles que se establecen en la plantilla de respuestas. Se capturan las respuestas predefinidas, la importancia de las preguntas asociadas, las notas y descripciones.
Revisor **Usuario de evaluación C3** (rol de usuario de IBM Data Risk Manager)	Revisar y validar evaluación	Ver respuestas tales como preguntas, notas y pruebas proporcionadas por los asesores en relación con las preguntas de la evaluación, realizar la validación y validar los informes de evaluación.

Crear un programa de evaluación

Utilice el componente Evaluación de IBM Data Risk Manager para crear un programa de evaluación para la evaluación.

Antes de empezar

Asegúrese de que se han creado las infraestructuras de evaluación necesarias, según sus requisitos, en el creador de infraestructuras. Para obtener más información sobre el Creador de infraestructuras, consulte “Creador de infraestructuras” en la página 181.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación .
3. Pulse **Evaluación**.

4. En la página **Evaluación**, seleccione un programa en la lista de programas. El ámbito y los límites para la evaluación se establecen como un programa basado en distintos factores, tales como unidades empresariales, plataformas, usuarios y roles.
5. En la sección **Lista de programas de evaluación**, pulse el icono **Crear programa de evaluación** ⊕.
6. En la página **Crear programa de evaluación**, establezca las opciones siguientes y pulse **Crear programa de evaluación**.

Opción	Descripción
Se puede compartir	Seleccione compartir o reutilizar las respuestas de este programa de evaluación con otras evaluaciones.
Nombre	El nombre de la evaluación.
Entorno	La infraestructura que se ha de utilizar para la evaluación. Las infraestructuras que se crean en el creador de infraestructuras están disponibles para su selección.
Entidad	Lista de entidades o nombres de dominio en evaluaciones no PRA. Seleccione entidades de negocio o nombres de dominio para definir el ámbito de las evaluaciones no PRA. El uso de ámbitos en la evaluación garantiza la recopilación de los datos necesarios de un forma eficaz y eficiente para evaluar riesgos.
Fecha de inicio, duración, unidad	**Fecha de inicio** Fecha de inicio de evaluación. **Duración** Duración de la evaluación. **Unidad** Unidad de medida, por ejemplo, `Día`, `Semana` o `Mes`.
Descripción	La descripción de la evaluación.
Objetivos	Finalidad y objetivo de la evaluación.
Departamento	Nombre de departamento de la organización donde se está realizando el programa de evaluación.
Línea de negocio	La línea de negocio asociada a la evaluación.
Clasificación de seguridad	La clasificación de seguridad del activo de información.
ID de riesgo global	Número de identificación de riesgo global correlacionado con ofertas de servicio relevantes.

Qué hacer a continuación
Cree una evaluación. Para ver los pasos para crear una evaluación, consulte "Creación de una evaluación para la infraestructura GDPR" en la página 192 y "Crear una evaluación para la infraestructura no GDPR" en la página 193.

Creación de una evaluación para la infraestructura GDPR

Para crear una evaluación, se pueden utilizar las cinco evaluaciones generadas para la infraestructura GDPR (infraestructura PRA).

Procedimiento

1. Cree un programa de evaluación seleccionando la infraestructura GDPR (infraestructura PRA) para crear la evaluación. Para ver los pasos para crear un programa de evaluación, consulte "Crear un programa de evaluación" en la página 191.
2. Cuando se crea un programa de evaluación con la infraestructura GDPR, de forma predeterminada, se muestran cinco evaluaciones GDPR en la página **Crear evaluación** para crear la evaluación para la infraestructura GDPR.

   Puede excluir una evaluación predeterminada de la lista al crear la evaluación. Para excluir, seleccione una evaluación y pulse el icono excluir .
3. Pulse **Crear evaluación**.

Qué hacer a continuación

Asigne recursos a la evaluación que ha creado. Para ver los pasos para asignar recursos, consulte "Asignar recursos para la evaluación" en la página 194.

Crear una evaluación para la infraestructura no GDPR

Utilice el componente Evaluación de IBM Data Risk Manager para crear una evaluación utilizando una infraestructura no GDPR (infraestructura no PRA) como, por ejemplo, la infraestructura para ISO 27002.

Acerca de esta tarea

En función de la selección de infraestructura durante la creación del programa de evaluación, se llenarán los temas asociados, subtemas y factores. Cada uno de los temas seleccionados forma una evaluación. Para obtener más información sobre cómo crear una infraestructura, consulte "Creador de infraestructuras" en la página 181.

Se pueden asociar entidades con sus conceptos a cada una de las evaluaciones según las necesidades de negocio. Se puede definir el ámbito de la evaluación en términos de dominios o entidades de negocio como, por ejemplo, procesos de negocio, aplicaciones y activos. El uso de ámbitos en la evaluación garantiza la recopilación de los datos necesarios de un forma eficaz y eficiente para evaluar riesgos.

El riesgo se calcula en función de diversos factores como, por ejemplo, la importancia de una determinada pregunta, la respuesta asociada, los activos asignados y su importancia (clasificación), amenazas y eventos correlacionados, y otros criterios definidos como parte de la personalización del cuestionario. Para obtener más información sobre cómo crear una pregunta, consulte "Creador de cuestionario" en la página 183.

Procedimiento

1. Cree un programa de evaluación seleccionando una infraestructura no GDPR (infraestructura no PRA) como, por ejemplo, la infraestructura ISO, para crear la evaluación. Para ver los pasos para crear un programa de evaluación, consulte "Crear un programa de evaluación" en la página 191.

   En la página **Crear evaluación** se muestran los temas, los subtemas y los factores asociados con la infraestructura que ha seleccionado.
2. Seleccione temas y subtemas de la lista.
3. Incluya entidades y conceptos para cada una de las evaluaciones (temas) que ha seleccionado.

   a) Pulse el icono **Editar evaluación** .

   b) Seleccione las entidades necesarias. De forma predeterminada, se seleccionan todas las entidades.

   c) Para cada una de las entidades seleccionadas, asocie los ámbitos necesarios. Para seleccionar conceptos, pulse el icono **Seleccionar ámbito** .

   d) Para guardar los cambios, pulse el icono Guardar .

4. Pulse **Crear evaluación**.

Qué hacer a continuación
Asigne recursos a la evaluación que ha creado. Para ver los pasos para asignar recursos, consulte "Asignar recursos para la evaluación" en la página 194.

Asignar recursos para la evaluación

Asigne recursos para ejecutar diferentes tareas relacionadas con las evaluaciones.

Acerca de esta tarea
Los recursos se asignan a los roles siguientes.

Administrador
Crea los programas de evaluación, las evaluaciones individuales dentro de un programa, las plantillas de evaluación y las preguntas relacionadas, asigna usuarios para proporcionar respuestas a las evaluaciones.

Asesor
Proporciona respuestas a las evaluaciones individuales de un programa.

Aprobador
Revisa y aprueba las respuestas de la evaluación.

Mediante la función de gestión de usuarios de IBM Data Risk Manager, los administradores pueden crear usuarios, asignar roles de usuario, actualizar la información de usuario y cambiar una contraseña de usuario. Para obtener más información acerca de la gestión de usuarios, consulte "Gestión de usuarios" en la página 96.

Procedimiento

1. Cree un programa de evaluación. Para ver los pasos para crear un programa de evaluación, consulte "Crear un programa de evaluación" en la página 191.
2. Crear una evaluación. Para ver los pasos sobre cómo crear una evaluación, consulte "Creación de una evaluación para la infraestructura GDPR" en la página 192 o "Crear una evaluación para la infraestructura no GDPR" en la página 193.
3. En la página **Asignar recurso**, seleccione los recursos en la lista **Asignar recurso** para asignar roles de usuario, tales como Administrador, Asesor y Aprobador.
4. Seleccione **Asignar recursos a todas las evaluaciones** para asignar los recursos seleccionados para todas las evaluaciones individuales.
5. Pulse **Asignar rol**.

Qué hacer a continuación
Ejecute las tareas de evaluación. Para ver los pasos sobre cómo ejecutar una evaluación, consulte "Realización de una evaluación" en la página 194.

Realización de una evaluación

El usuario con el rol de Asesor debe proporcionar las respuestas para los cuestionarios de evaluación. Una vez proporcionadas las respuestas a las preguntas, el asesor envía la evaluación al aprobador para que lo revise y lo apruebe.

Antes de empezar

- Se crea un programa de IBM Data Risk Manager con el ámbito definido y se proporciona a los usuarios acceso al programa.
- Se crean los usuarios con los privilegios adecuados en IBM Data Risk Manager.

- Asigne el rol de `Administrador BCM` a los usuarios designados como administradores del programa de evaluación.
- Asigne el rol `Evaluación general C3` a los usuarios designados para proporcionar respuestas a una evaluación.

Acerca de esta tarea

Las respuestas a algunas preguntas llevan a preguntas adicionales. Puede expresar esta relación creando una relación condicional entre preguntas. En una relación condicional, hay una pregunta padre y una respuesta hijo. De forma predeterminada, la pregunta hijo no se visualiza. La pregunta hijo se visualiza solo cuando se proporciona una respuesta habilitadora a la pregunta padre. Mediante el árbol de decisiones, puede ver e identificar rápidamente las relaciones entre las preguntas.

El árbol de decisiones es una estructura jerárquica con nodos y bordes dirigidos. Un árbol de decisiones normalmente se inicia con un solo nodo (pregunta padre), que se ramifica (preguntas hijo) en los posibles resultados. Cada uno de estos resultados puede llevar a nodos adicionales, que se ramifican en otras posibilidades. Esto le da una estructura similar a un árbol. Mediante un árbol de decisiones, puede explicar fácilmente las decisiones, identificar posibles sucesos que podrían producirse y ver los posibles resultados.

Para las evaluaciones no PRA, cuando se proporcionan respuestas a una pregunta, los datos de contexto se pueden capturar en función de las entidades definidas (ámbitos) para el cálculo de puntuación de riesgo. Para obtener más información sobre cómo definir entidades y asociarlas a las evaluaciones, consulte "Crear un programa de evaluación" en la página 191 y "Crear una evaluación para la infraestructura no GDPR" en la página 193.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) utilizando sus credenciales de asesor.
2. Pulse el icono de notificaciones para visualizar el panel de control de mensajes.

   Las notificaciones incluyen un enlace con el programa de evaluación o con la evaluación individual para la que se proporcionan las respuestas.
3. Como alternativa, pulse el icono del menú de aplicaciones .
4. Pulse **Evaluación**.
5. Seleccione el programa de evaluación de **Lista de programas de evaluación**. Se muestra una lista de evaluaciones asociadas con el programa de evaluación en la sección **Evaluaciones**.
6. Seleccione la evaluación para la que debe proporcionar respuestas.

   La lista siguiente proporciona más información para realizar la evaluación.

   - Pulse el icono **Asignar recurso** para asignar recursos.
   - Pulse el icono **Calcular puntuación de evaluación** para calcular la puntuación para evaluaciones no PRA.
   - Pulse el icono **Notas** para añadir una nota sobre la evaluación.
   - Pulse el icono **Importar evaluación** para importar respuestas desde una evaluación completada. Después de importar una respuesta de evaluación, se bloquea la evaluación y no se puede editar.

     Está disponible un programa de evaluación para compartirlo solo después de que se haya validado y la opción **Se puede compartir** está seleccionada cuando se crea el programa de evaluación.
   - Pulse el icono **Suprimir evaluación** para suprimir la evaluación seleccionada.

- Pulse el icono **Gestionar ámbito**  para añadir o modificar la selección del ámbito para las evaluaciones no PRA.

  Puede modificar y gestionar la selección del ámbito que ha definido durante la creación de la evaluación. Solo el propietario del programa de evaluación o el creador de la evaluación puede modificar la selección del ámbito. Puede modificar la selección del ámbito solo para las evaluaciones con un estado de `En curso`, `En pausa` y `Completado`.

- El icono asignado  indica que usted es el Asesor de la evaluación.

7. Pulse **Iniciar evaluación** para iniciar la evaluación.
8. Los elementos de registro se muestran en el panel de la izquierda. Seleccione un elemento de registro en la lista. Se muestran las preguntas asociadas.

   Pulse el icono  para excluir el elemento de registro seleccionado de la evaluación. Cuando se excluye un elemento de registro de la evaluación, el asesor no puede volver a incluir el elemento. El aprobador puede volver a incluir este elemento, si es necesario.

   Para las evaluaciones no PRA, el icono **Contexto** se muestra para seleccionar la información de contexto. Pulse el icono de contexto para seleccionar el contexto en el nivel (control) de elemento de registro. Se puede aplicar la misma información de contexto a todas las preguntas asociadas.

   - Pulse **Vista de cuadrícula** para ver las preguntas y respuestas de la evaluación en formato de cuadrícula (vista predeterminada).
   - Pulse **Vista de lista** para ver las preguntas y respuestas de la evaluación en formato de lista.

9. Seleccione una pregunta y especifique la respuesta, las notas y la observación sobre la respuesta.

   Pulse el icono más opciones para proporcionar la información siguiente.

   - Pulse en **Notas** para añadir una nota a la respuesta.
   - Pulse **Observación** para seleccionar las observaciones a las respuestas.

10. Añada los detalles siguientes para las preguntas.

    - Pulse en el icono **Notas**  para añadir una nota a la pregunta.
    - Pulse el icono **Seguimientos de auditoría**  para ver los seguimientos de auditoría.
    - Si desea restablecer un valor de respuesta, pulse el icono **Restablecer**  en los valores predeterminados.
    - Para las evaluaciones no PRA, pulse el icono **Contexto**  para añadir o actualizar la información de contexto.

      El icono **Contexto** se muestra solo después de que se haya proporcionado una respuesta a la pregunta. Seleccione los contextos y guarde la información basándose en sus necesidades. Si los contextos ya están seleccionados en el nivel de control, puede modificar los detalles si es necesario.

11. Especifique respuestas a todas las preguntas.
12. Pulse **Enviar para revisión** para enviar la evaluación para la revisión para validar las respuestas.
13. Pulse **Sí** en la ventana de confirmación.

    Después de enviar la evaluación para la revisión, no se pueden realizar cambios en las respuestas hasta que el aprobador de la evaluación valide las respuestas.

Qué hacer a continuación

Cuando se completa la revisión y la aprobación de las respuestas de la evaluación, se notifica al aprobador. Si es necesario, el aprobador puede añadir comentarios y devolverlos al asesor para realizar

modificaciones adicionales. Para obtener más información acerca de cómo aprobar las respuestas, consulte “Completar la revisión y aprobación de las respuestas de la evaluación” en la página 197.

Completar la revisión y aprobación de las respuestas de la evaluación

El aprobador debe revisar y aprobar las respuestas de la evaluación. Si es necesario, el aprobador puede añadir comentarios de revisión y devolverlos al asesor para realizar modificaciones adicionales.

Antes de empezar

- Se crea un programa de IBM Data Risk Manager con el ámbito definido y se proporciona a los usuarios acceso al programa.
- Se crean los usuarios con los privilegios adecuados en IBM Data Risk Manager.
  - Asigne el rol de `Administrador BCM` a los usuarios designados como administradores del programa de evaluación.
  - Asigne el rol `Evaluación general C3` a los usuarios designados para proporcionar respuestas a una evaluación.

Acerca de esta tarea

Las respuestas a algunas preguntas llevan a preguntas adicionales. Puede expresar esta relación creando una relación condicional entre preguntas. En una relación condicional, hay una pregunta padre y una respuesta hijo. De forma predeterminada, la pregunta hijo no se visualiza. La pregunta hijo se visualiza solo cuando se proporciona una respuesta habilitadora a la pregunta padre. Mediante el árbol de decisiones, puede ver e identificar rápidamente las relaciones entre las preguntas.

El árbol de decisiones es una estructura jerárquica con nodos y bordes dirigidos. Un árbol de decisiones normalmente se inicia con un solo nodo (pregunta padre), que se ramifica (preguntas hijo) en los posibles resultados. Cada uno de estos resultados puede llevar a nodos adicionales, que se ramifican en otras posibilidades. Esto le da una forma similar a un árbol. Mediante un árbol de decisiones, puede explicar fácilmente las decisiones, identificar posibles sucesos que podrían producirse y ver los posibles resultados.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) utilizando sus credenciales de aprobador.
2. Pulse el icono de notificaciones para visualizar el panel de control de mensajes.

   Las notificaciones incluyen un enlace con el programa de evaluación o con la evaluación individual para la que se proporcionan las respuestas.
3. Como alternativa, pulse el icono del menú de aplicaciones .
4. Pulse **Evaluación**.
5. En la sección **Lista de programas de evaluación**, seleccione la evaluación que deba revisar y proporcione comentarios de revisión.
6. Pulse el icono **Iniciar evaluación** para abrir la página de evaluación para revisar las respuestas y añadir comentarios de revisión. De forma predeterminada, se muestran todas las preguntas con respuestas. También puede ver las preguntas en función del grupo asociado con la pregunta.
   - Pulse **Vista de cuadrícula** para ver las preguntas y respuestas de la evaluación en formato de cuadrícula (vista predeterminada).
   - Pulse **Vista de lista** para ver las preguntas y respuestas de la evaluación en formato de lista.
7. Revise las respuestas a todas las preguntas.
   - Pulse el icono **Notas** para ver los comentarios sobre una pregunta.

- Pulse el icono **Seguimientos de auditoría** para ver la información de seguimiento de auditoría.
- Pase el cursor sobre **Respondida** para ver la puntuación calculada de una pregunta específica.
- Pulse el icono **Revisar comentarios** para añadir comentarios de revisión.
- Pulse el icono **Más opciones** para ver información de respuestas.
  - Pulse el icono **Notas** para ver la nota que se ha añadido al proporcionar las respuestas.
  - Pulse el icono **Observación** para ver los datos de observación.

.

8. Para ver todos los comentarios de un revisor o asesor para una evaluación, habilite el conmutador **Modo de comentario** y pulse **Comentarios**.
   - Pulse **Historial** para ver todos los comentarios del descriptor de acceso o del revisor.
   - Pulse **Hoja de revisión** para aceptar o rechazar los comentarios.
9. Si necesita enviar la evaluación al asesor para realizar más modificaciones, pulse **Volver a asesor**.
10. Pulse **Completar revisión** para completar el proceso de revisión.
11. En la ventana **Completar revisión**, proporcione sus comentarios sobre la finalización de la revisión.
12. Pulse **Enviar**.
13. Pulse **Aceptar** en la ventana **Información**.

Qué hacer a continuación

Una vez completado el proceso de revisión, el aprobador puede validar para completar la evaluación. Para ver los pasos sobre cómo validar, consulte "Validación de un programa de evaluación" en la página 198.

Validación de un programa de evaluación

El aprobador debe validar para completar la evaluación.

Antes de empezar

Asegúrese de revisar que se han completado las respuestas de la evaluación.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) utilizando sus credenciales de aprobador.
2. Pulse el icono de notificaciones para visualizar el panel de control de mensajes.
   Las notificaciones incluyen un enlace con el programa de evaluación o con la evaluación individual para la que se proporcionan las respuestas.
3. Como alternativa, pulse el icono del menú de aplicaciones.
4. Pulse **Evaluación**.
5. En la sección **Lista de programas de evaluación**, seleccione la evaluación que debe validar.
6. Pulse el icono **Más opciones** y a continuación pulse **Validar**.
7. En la ventana **Programa de validación de evaluación**, proporcione los comentarios sobre la validación de la evaluación.
8. Pulse **Enviar** para completar el proceso de validación.

Visualización del informe de puntuación de evaluación

Los resultados de las evaluaciones independientes generan un informe de evaluación de riesgos basado en las respuestas obtenidas. En el panel de instrumentos Evaluaciones, se puede ver la información de evaluación en formatos gráfico y tabular. La representación gráfica de los datos le ayuda a comprender e interpretar fácilmente la información.

Acerca de esta tarea

Se pueden descargar informes para el registro de activos de información, los controles de vulnerabilidades y la evaluación de riesgos.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) utilizando sus credenciales de aprobador.
2. Pulse el icono de notificaciones para visualizar el panel de control de mensajes.

   Las notificaciones incluyen un enlace con el programa de evaluación o con la evaluación individual para la que se proporcionan las respuestas.
3. Como alternativa, pulse el icono del menú de aplicaciones .
4. Pulse **Evaluación**.
5. Para ver el informe de evaluación de infraestructura GDPR (PRA), siga los pasos siguientes.
   a) Seleccione el programa de evaluación de **Lista de programas de evaluación**.
   b) Seleccione la evaluación completada para la que desea ver el informe.
   c) Pulse la pestaña **Informe**.
   d) Pulse el icono **Renovar vista** para renovar la lista para visualizar el informe gráfico para la evaluación seleccionada.
   e) Pulse el icono **Conmutar vista de gráfico/cuadrícula** para visualizar información sobre la evaluación en formato tabular.
   f) Para la vista expandida, pulse el icono **Expandir/Contraer** .
   g) Para configurar las acciones de corrección de riesgo, ejecute los pasos siguientes.
      1) Pulse la pestaña **Evaluación de riesgo**.
      2) Seleccione un riesgo.
      3) Pulse el icono **Actualizar acción** para seleccionar una acción para remediar los riesgos.
      4) Pulse el icono **Crear actividad** para definir las acciones de corrección de riesgo. Para obtener información sobre cómo crear actividades y tareas en el Centro de acción, consulte “Creación de una actividad de reparación ” en la página 153.
   h) Pulse **Descargar informe** para descargar los informes para **Evaluación de riesgo**, **Registro de activos de información** y **Controles de vulnerabilidad**.
6. Para ver el informe para la evaluación de infraestructura no GDPR, ejecute los pasos siguientes.
   a) Seleccione el programa de evaluación de **Lista de programas de evaluación**.
   b) Seleccione la evaluación completada para la que desea ver el informe.
   c) Pulse el icono **Calcular puntuación de evaluación** .
   d) Pulse la pestaña **Informe**.
   e) Pulse el icono **Renovar vista** para renovar la lista para visualizar el informe gráfico para la evaluación seleccionada.

f) Pulse el icono **Conmutar vista de gráfico/cuadrícula** para  visualizar información sobre la evaluación en formato tabular.

g) Para la vista expandida, pulse el icono **Expandir/Contraer**  .

Qué hacer a continuación

En el caso de una evaluación no PRA, también puede ver el informe de evaluación basado en el ámbito para los ámbitos que se definen cuando se crea el programa de evaluación. Para obtener más información sobre cómo ver el informe, consulte "Visualización del informe de puntuación basado en ámbito" en la página 200.

Visualización del informe de puntuación basado en ámbito

En el panel de control Evaluación, puede ver los resultados de las evaluaciones independientes que se han realizado en una infraestructura en función de unos ámbitos establecidos (entidades de negocio) que haya definido. La representación gráfica de los datos le ayuda a comprender e interpretar fácilmente la información.

Acerca de esta tarea

Para las evaluaciones no PRA, cuando se proporcionan respuestas a una pregunta, los datos de contexto se pueden capturar en función de las entidades definidas (ámbitos) para el cálculo de puntuación de riesgo. Para obtener más información sobre cómo definir entidades y asociarlas a las evaluaciones, consulte "Crear un programa de evaluación" en la página 191 y "Crear una evaluación para la infraestructura no GDPR" en la página 193.El uso de ámbitos en la evaluación garantiza la recopilación de los datos necesarios de un forma eficaz y eficiente para evaluar riesgos.

La puntuación de riesgo en el informe representa la puntuación media de los controles para los ámbitos definidos.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) utilizando sus credenciales de aprobador.
2. Pulse el icono de notificaciones  para visualizar el panel de control de mensajes.

   Las notificaciones incluyen un enlace con el programa de evaluación o con la evaluación individual para la que se proporcionan las respuestas.
3. Como alternativa, pulse el icono del menú de aplicaciones  .
4. Pulse **Evaluación**.
5. Seleccione el programa de evaluación de **Lista de programas de evaluación**. El informe de evaluación basado en ámbito solo se puede visualizar en el caso de una infraestructura no PRA.
6. Seleccione la evaluación completada para la que desea ver el informe.
7. Pulse el icono **Calcular puntuación de evaluación**  .
8. Pulse en la pestaña **Informe basado en ámbito**.

   Las pestañas aparecen en las entidades definidas durante la creación del programa de evaluación para ver los datos de evaluación basados en ámbito. Por ejemplo, Procesos de negocio, Aplicaciones u Orígenes de datos.
9. Para ver el informe para la entidad de proceso de negocio, pulse la pestaña **Procesos de negocio**.
10. Para ver el informe para l entidad de aplicación, pulse la pestaña **Aplicaciones**.
11. Para ver el informe para la entidad del origen de datos, pulse la pestaña **Orígenes de datos**.

Gestión de resultados de evaluación

Basándose en los resultados de evaluación PRA, las acciones apropiadas se pueden implementar para abordar y mitigar los riesgos identificados. Puede utilizar el módulo Gestión del resultado de evaluación de IBM Data Risk Manager para ver y gestionar los riesgos.

Adición de un riesgo

Puede crear riesgos, definir sus atributos y añadir planes de reparación para un ámbito basándose en la puntuación de riesgo que se ha generado después de que se haya completado la evaluación de riesgo de una evaluación no PRA. Se pueden añadir varios riesgos a un ámbito.

Acerca de esta tarea

Puede importar atributos de riesgo desde el inventario de amenazas de IBM Data Risk Manager. Para obtener más información sobre el inventario de amenazas, consulte “Inventario de amenazas ” en la página 131.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) utilizando sus credenciales de aprobador.
2. Pulse el icono de menú de aplicación  .
3. Pulse **Evaluación**.
4. Seleccione un programa de evaluación para una infraestructura no PRA desde **Lista de programas de evaluación**.
5. Pulse el icono **Gestión de resultados de evaluación**  .
6. Seleccione un ámbito en la lista.
7. Pulse **Añadir riesgo**.
8. En la ventana **Añadir riesgo**, establezca las opciones siguientes.
   a) Especifique los atributos de riesgo.

Nombre del riesgo	Especifique un nombre para el riesgo.
Categoría	Especifique la categoría a la que pertenece el riesgo.
Tipo de riesgo	Especifique la clasificación del riesgo.
Gravedad	Especifique el nivel de gravedad del riesgo.
Nivel de impacto	Especifique el nivel del impacto de riesgo: bajo, medio o alto.
Probabilidad	Especifique la probabilidad de que se produzcan los riesgos.
Descripción del riesgo	Añada una descripción del riesgo.

   b) De forma alternativa, puede importar atributos de riesgo desde el repositorio de amenazas de IBM Data Risk Manager.
      1) Pulse **Repositorio de amenazas**.
      2) Seleccione una amenaza en la lista.
   c) Especifique los atributos de ámbito.

Estado	Especifique el estado del riesgo.
Excepción solicitada	Especifique la información de excepción para la conformidad.
Fecha límite para el arreglo	Especifique la fecha de mitigación del riesgo planificado.
Fecha de mitigación	Especifique la fecha de mitigación del riesgo real.

Mitigación	Especifique la información de mitigación del riesgo.
Observaciones sobre el riesgo	Especifique observaciones sobre el riesgo.

9. Pulse **Guardar**.

Qué hacer a continuación
Añada una actividad de reparación para el riesgo que acaba de crear. Para ver los pasos sobre cómo crear una actividad, consulte "Creación de un plan de acción para reparar riesgos " en la página 202.

Creación de un plan de acción para reparar riesgos

Puede añadir actividades de reparación para los riesgos de evaluación identificados.

Antes de empezar
Asegúrese de que se ha completado la evaluación, se ha generado la puntuación de riesgo y se han identificado los riesgos para los ámbitos. Para ver los pasos sobre cómo añadir riesgos, consulte "Adición de un riesgo " en la página 201.

Acerca de esta tarea
Puede utilizar actividades de reparación predefinidas y las tareas importadas de un paquete de soluciones para definir planes de acción. Pulse el icono de actividades predefinidas  para seleccionar las actividades predefinidas.

Procedimiento

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<Dirección-IP-Servidor IDRM>:8443/albatross/a3suite`) utilizando sus credenciales de aprobador.
2. Pulse el icono de menú de aplicación  .
3. Pulse **Evaluación**.
4. Seleccione un programa de evaluación para una infraestructura no PRA desde **Lista de programas de evaluación**.
5. Pulse el icono **Gestión de resultados de evaluación**  .
6. Seleccione un ámbito en la lista. Los riesgos asociados se muestran en **Riesgos identificados**.
7. Seleccione un riesgo para el cual debe crear una actividad.
8. Pulse **Añadir actividad**.
9. En la ventana **Crear actividad de reparación**, especifique los detalles necesarios.

Opción	Descripción
Nombre de actividad	Especifique el nombre de la actividad.
Estado	Especifique el estado de la actividad, por ejemplo, `Por iniciar`, `En curso` o `Completada`.
Operación de actividad	Seleccione una actividad de operación en la lista.
Riesgo asociado	Seleccione un origen de datos en el inventario de orígenes de datos para el cual debe crear una actividad de reparación. Solo puede asignar un origen de datos como ámbito a una actividad.
Fecha de inicio	Especifique la fecha para iniciar la actividad de reparación.

Opción	Descripción
Fecha de finalización	Especifique la fecha para finalizar la actividad de reparación.
Duración	Especifica la duración entre la fecha de inicio y finalización de la actividad.
Impacto	Especifique el nivel del impacto de riesgo: bajo, medio o alto.
Urgencia	Especifique el nivel de urgencia para abordar el riesgo.
Prioridad	Especifique el nivel de prioridad en el cual se debe resolver el riesgo, basándose en el impacto y la urgencia.
Gravedad	Especifique el nivel de gravedad del riesgo.
Subcategoría	Especifique la subcategoría del riesgo.
Descripción	Añada una descripción del riesgo.
Categoría	Especifique la categoría a la que pertenece el riesgo.
Tipo de contacto	Especifique el tipo de contacto.
Recursos asignados	Especifique el propietario del riesgo.

10. Para guardar los detalles de actividad, pulse **Crear**.

Qué hacer a continuación
Edite y gestione más la actividad que ha creado con más detalles en el componente Centro de acción de IBM Data Risk Manager. En el Centro de acción, puede ver y acceder a la actividad en **Proyecto de reparación de riesgo** para las modificaciones. Para obtener más información sobre el Centro de acción, consulte “Centro de acción” en la página 151.

Herramientas de diagnóstico

Las herramientas de diagnóstico están disponibles para ayudarle a identificar problemas y a resolver problemas que se encuentran cuando está trabajando con IBM Data Risk Manager.

Herramienta de diagnóstico de integración

IBM Data Risk Manager incluye una herramienta de diagnóstico que se puede utilizar para ayudar a la determinación de problemas.

La herramienta de diagnóstico de integración de IBM Data Risk Manager ayuda en la resolución de problemas de base de datos y de conectividad de integración.

1. Abra un indicador de mandatos /terminal.
2. SSH en IBM Data Risk Manager.
3. Ejecute el mandato siguiente.

```
cd ~/Diagnostics
java -jar a3IntegrationDiagnostics.jar
```

4. Se muestra la salida siguiente para que seleccione una opción.

```
Bienvenido a iDRM Diagnostics Tool
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Escriba una entrada válida
 Las siguientes son las opciones.
 1. Integración
```

```
2. Origen de datos
3. Salir
```

5. Para identificar y resolver los problemas de integración, escriba 1 y pulse **Intro**.
6. Para identificar y resolver los problemas de conectividad de base de datos, escriba 2 y pulse **Intro**.

Nota: para obtener más información sobre los errores que se notifican, compruebe los archivos de registro.

Herramienta de diagnóstico de estado

IBM Data Risk Manager incluye una herramienta de diagnóstico de estado que se puede utilizar para ayudar a la determinación de problemas.

La herramienta de diagnóstico de estado de IBM Data Risk Manager le ayuda a supervisar el estado del servidor, el estado del agente, el estado de validez de la licencia, el estado del parche y la validez de la generación de señales OAuth.

1. Abra un indicador de mandatos /terminal.
2. SSH en IBM Data Risk Manager.
3. Ejecute el mandato siguiente.

```
cd ~/Diagnostics
java -jar a3HealthDiagnostics.jar
```

4. Se muestra la salida siguiente para que seleccione una opción.

```
Bienvenido a iDRM Health Diagnostics
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Estas son las opciones. Especifique una opción válida.
Pulse 1 para comprobar el estado del servidor
Pulse 2 para comprobar el estado de los microservicios
Pulse 3 para comprobar si está actualizada la licencia
Pulse 4 para comprobar la generación de señales oauth
Pulse 5 para comprobar el estado del parche
Pulse 6 para salir
```

5. Escriba el número que se visualiza junto a su elección y pulse **Intro**.

Nota: para obtener más información sobre los errores que se notifican, compruebe los archivos de registro.

Resolución de problemas y soporte

La información de resolución de problemas y soporte de IBM Data Risk Manager le ayuda a entender, aislar y resolver problemas.

La sección de resolución de problemas incluye descripciones de los sucesos que han generado problemas, los síntomas, el entorno, las causas posibles y las recomendaciones para las acciones de recuperación.

La sección de soporte proporciona información acerca de las herramientas y las opciones que puede utilizar para conectar con la organización de servicio y soporte. La sección de soporte también incluye información general acerca de cómo realizar búsquedas en las bases de conocimientos, obtener arreglos y contactar con el soporte de IBM, además de temas específicos del producto.

Para resolver un problema por sí mismo, puede averiguar cómo identificar el origen de un problema, cómo reunir información de diagnóstico, dónde obtener arreglos y en qué bases de conocimientos buscar. Si tiene que ponerse en contacto con el soporte de IBM, puede averiguar la información de diagnóstico que los técnicos de servicio necesitan para ayudarle a resolver el problema.

Información general

Para comenzar a utilizar la resolución de problemas, debe familiarizarse con las técnicas básicas de resolución de problemas y cómo ponerse en contacto e intercambiar información con el soporte de IBM. También puede utilizar las herramientas, como IBM Knowledge Base, Fix Central y Support Portal.

Técnicas para la resolución de problemas

La *resolución de problemas* es un método sistemático para solucionar un problema. El objetivo de la resolución de problemas es determinar por qué algo no funciona del modo esperado y cómo resolverlo. Algunas técnicas comunes pueden ayudar con la tarea de resolución de problemas.

El primer paso del proceso de resolución de problemas es describir el problema completamente. Las descripciones de problemas le ayudan a usted y al representante del soporte técnico de IBM a determinar por dónde comenzar para encontrar la causa del problema. Este paso incluye la formulación de preguntas 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 evidente es "¿Cuál es el problema?" Esta pregunta puede resultar demasiado directa, sin embargo, puede subdividirse en varias preguntas más focalizadas que crean una imagen más descriptiva del problema. Estas preguntas pueden ser:

- ¿Quién, o qué, informa del problema?
- ¿Cuáles son los códigos y mensajes de error?
- ¿Cómo se produce el error en el sistema? Por ejemplo, ¿se trata de un bucle, un bloqueo, una degradación del rendimiento o un resultado incorrecto?

¿Dónde se produce el problema?

Determinar dónde se origina el problema no siempre es fácil, pero es uno de los pasos más importantes para resolver un problema. Muchas capas de tecnología pueden existir entre los componentes de informe y los componentes anómalos. Las redes, discos y controladores son únicamente algunos de los componentes que se han de tener en cuenta cuando se investigan problemas.

Las siguientes preguntas le ayudarán a centrarse en dónde se produce el problema para aislar la capa del problema:

- ¿El problema es específico de una plataforma o sistema operativo o es común en varias plataformas o sistemas operativos?
- ¿Están admitidos el entorno y la configuración actuales?
- ¿Todos los usuarios tienen el mismo problema?
- (Para instalaciones en varios sitios). ¿Todos los sitios tienen el problema?

Si una capa informa del problema, el problema no tiene por qué haberse generado necesariamente en esa capa. Para poder identificar dónde se origina un problema, es necesario 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 utilizando un entorno cuya configuración está soportada;

muchos problemas se producen por niveles incompatibles de software que no están diseñados para funcionar conjuntamente o no se han probado conjuntamente de forma exhaustiva.

¿Cuándo se produce el problema?

Desarrolle una línea temporal detallada de sucesos que den como resultado un error, especialmente para los casos que sólo ocurran una vez. Puede desarrollar fácilmente una línea de tiempo trabajando hacia atrás: empiece en el momento de informar del error (lo más preciso posible, incluso hasta el milisegundo) y siga hacia atrás mediante los registros e información disponibles. Normalmente solo deberá llegar hasta el primer suceso sospechoso que encuentre en un registro de diagnóstico.

Para desarrollar una línea temporal detallada de sucesos, responda a estas preguntas:

- ¿El problema se produce solo en un momento determinado del día o de la noche?
- ¿Con qué frecuencia sucede el problema?
- ¿Qué secuencia de sucesos antecede al momento en que se informa del problema?
- ¿Sucede el problema después de un cambio de entorno como, por ejemplo, la actualización o instalación de software o hardware?

La respuesta a este tipo de preguntas puede proporcionar un marco de referencia en el que investigar el problema.

¿En qué condiciones se produce el problema?

Saber qué sistemas y aplicaciones se están ejecutando en el momento en que se produce un problema es una parte importante de la resolución de problemas. Estas preguntas sobre el entorno le ayudarán a identificar la causa raíz del problema:

- ¿El problema se produce siempre cuando se realiza la misma tarea?
- ¿Debe producirse una determinada secuencia de sucesos para que ocurra el problema?
- ¿Fallan otras aplicaciones al mismo tiempo?

La respuesta a este tipo de preguntas le ayudará a conocer el entorno en el que se produce el problema y establecer correlaciones de dependencias. Recuerde que simplemente porque se producen los problemas a la misma hora, no significa que los problemas estén 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. Normalmente, cuando un problema se puede reproducir, dispone de un conjunto de herramientas o procedimientos mayor para ayudarle en la investigación. Por lo tanto, los problemas que puede reproducir suelen ser más fáciles de depurar y resolver.

No obstante, los problemas que puede reproducir pueden tener una desventaja: si el problema tiene un impacto empresarial importante, no desea que se repita. Si es posible, vuelva a crear el problema en un entorno de prueba o desarrollo, que generalmente ofrece más flexibilidad y control durante la investigación.

- ¿Se puede recrear el problema en un sistema de prueba?
- ¿Hay varios usuarios o aplicaciones que tengan el mismo tipo de problema?
- ¿Se puede recrear el problema ejecutando un solo mandato, un conjunto de mandatos o una aplicación concreta?

Búsqueda en las 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 realizando búsquedas en la documentación de IBM Data Risk Manager. No obstante, en ocasiones tiene que buscar en otras ubicaciones más allá de la documentación para encontrar una respuesta a sus preguntas o para resolver problemas.

Procedimiento

Para buscar la información que necesita en las bases de conocimiento, utilice uno o más de los siguientes métodos:

- Buscar contenido utilizando IBM Support Assistant (ISA).

  ISA es un entorno de trabajo de capacidad de servicio de software sin cargo que ayuda a responder preguntas y resolver problemas con los productos de software de IBM. Puede buscar instrucciones para descargar e instalar ISA en el sitio web de ISA.
- Busque el contenido que necesite utilizando IBM Support Portal.

  IBM Support Portal es una vista unificada y centralizada de todas las herramientas de soporte técnico y la información de todos los sistemas, el software y los servicios de IBM. IBM Support Portal le permite acceder a la cartera de productos de soporte electrónico de IBM desde un único sitio. Puede adaptar las páginas para centrarse en la información y los recursos que necesita para prevenir problemas y resolverlos más rápidamente. Estos vídeos ofrecen una introducción a la herramienta IBM Support Portal, exploran la resolución de problemas y otros recursos, y muestran cómo se puede personalizar la página, moviendo, añadiendo y suprimiendo portlets.
- Busque contenido acerca de IBM Data Risk Manager.
  - Sitio web de soporte de IBM Data Risk Manager.
- Busque contenido utilizando la búsqueda de encabezado de IBM.

  Puede utilizar la búsqueda de encabezado de IBM escribiendo la serie de búsqueda en el campo de **búsqueda** en la parte superior de cualquier página de ibm.com.
- Busque contenido utilizando cualquier motor de búsqueda externo, como Google, Yahoo o Bing.

  Si utiliza un motor de búsqueda externo, será más probable que los resultados incluyan información que no pertenezca al dominio de ibm.com. No obstante, en ocasiones puede encontrar información útil para resolver problemas acerca de los 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.

Obtención de arreglos de Fix Central

Puede utilizar Fix Central para buscar los arreglos proporcionados por el servicio de soporte IBM para una variedad de productos, incluido IBM Data Risk Manager. 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 un arreglo de producto disponible para resolver el problema.

Acerca de esta tarea

Procedimiento

Para buscar e instalar arreglos:

1. Consiga las herramientas necesarias para obtener el arreglo. Si no está instalado, obtenga el instalador de actualización del producto. Puede descargar el instalador desde Fix Central.

   Este sitio ofrece instrucciones de descarga, instalación y configuración para el instalador de actualización.
2. Seleccione IBM Data Risk Manager como el producto y marque uno o más recuadros de selección que sean relevantes para el problema que desea resolver.

Para obtener detalles, consulte: http://www.ibm.com/systems/support/fixes/en/fixcentral/help/faq_sw.html.

3. Identifique y seleccione el arreglo que necesita.
4. Descargue el arreglo.
   a) Abra el documento descargado y siga el enlace de la sección "Descargar paquete".
   b) Al descargar el archivo, asegúrese de que no se cambia el nombre del archivo de mantenimiento.
      Este cambio puede ser intencionado o puede ser un cambio inadvertido originado por determinados navegadores web o programas de utilidad de descarga.
5. Aplique el arreglo.
   a) Siga las instrucciones de la sección "Instrucciones de instalación" del documento de descarga.
   b) Para obtener más información, consulte el tema "Instalación de los arreglos con el instalador de actualización" en la documentación del producto.

Intercambio de información con IBM

Para diagnosticar o identificar un problema, es posible que deba proporcionar datos e información del sistema al soporte de IBM. En otros casos, el soporte de IBM puede proporcionar herramientas o programas de utilidad para utilizarlos en la determinación de problemas.

Envío de información al soporte de IBM

Con el fin de reducir el tiempo necesario para resolver su problema, puede enviar información de rastreo y diagnóstico al soporte de IBM.

Procedimiento

Para enviar información de diagnóstico al soporte de IBM:

1. Abra un registro de gestión de problemas (PMR).
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 manual o automáticamente:
   - Recopilar los datos manualmente.
   - Recopilar los datos automáticamente.
3. Comprima los archivos utilizando el formato de archivo `.zip` o `.tar`.
4. Transfiera los archivos a IBM.

   Puede utilizar uno de los métodos siguientes para transferir los archivos a IBM:

   - IBM Support Assistant
   - 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 sitio web de soporte de IBM.

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 utilizar FTP para descargar dichos archivos.

Antes de empezar

Asegúrese de que el representante de soporte técnico de IBM le haya proporcionado los datos del servidor específico que deberá utilizar para descargar los archivos, así como el directorio exacto y los nombres de archivo a los que debe acceder.

Procedimiento

Para descargar los archivos del soporte de IBM:

1. Utilice FTP para conectarse al sitio que le ha indicado el representante de soporte técnico de IBM e inicie sesión como usuario `anónimo`. Utilice la dirección de correo electrónico como contraseña.
2. Vaya al directorio adecuado:
   a) Cambie al directorio `/fromibm`.

   ```
   cd fromibm
   ```

   b) Vaya al directorio que el representante del soporte técnico de IBM le ha proporcionado.

   ```
   cd nombre_directorio
   ```

3. Habilite la modalidad binaria para la sesión.

   ```
   binary
   ```

4. Utilice el mandato **get** para descargar el archivo que el representante de soporte técnico de IBM haya especificado.

   ```
   get filename.extension
   ```

5. Finalice la sesión FTP.

   ```
   quit
   ```

Suscripción a las 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

Si se suscribe para recibir actualizaciones sobre IBM Data Risk Manager, puede recibir información técnica importante y actualizaciones de recursos y herramientas de soporte de IBM. Puede suscribirse a las actualizaciones mediante uno de los procedimientos siguientes:

Canales de información RSS

Para obtener información sobre RSS, incluidos los pasos para empezar y una lista de páginas web de IBM habilitadas para RSS, visite el sitio de canales de información RSS de soporte de software de IBM Software.

Mis notificaciones

Con **Mis notificaciones**, puede suscribirse a las actualizaciones de soporte de cualquier producto de IBM. **Mis notificaciones** sustituyes a **Mi soporte**, que es una herramienta similar que puede que haya utilizado en el pasado. Con **Mis notificaciones**, puede especificar que desea recibir a diario o semanalmente anuncios de 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 categorizar los productos sobre los que desea ser informado y los métodos de entrega que mejor se adaptan a sus necesidades.

Procedimiento

Para suscribirse a las actualizaciones de soporte:

1. Para suscribirse a Mis notificaciones, vaya a IBM Support Portal y pulse **Mis notificaciones** en el portlet **Notificaciones**.
2. Inicie sesión utilizando su ID de usuario y contraseña de IBM, y pulse **Enviar**.
3. Identifique qué actualizaciones desea recibir y cómo desea recibirlas.

a) Pulse la pestaña **Subscribe**.

b) Seleccione la marca de software o el tipo de hardware adecuados.

c) Seleccione uno o más productos por su nombre y pulse **Continuar**.

d) Seleccione sus preferencias sobre cómo recibir actualizaciones: por correo electrónico, en línea en una carpeta designada o como un canal de información RSS o Atom.

e) Seleccione los tipos de actualizaciones de documentación que desea recibir, por ejemplo información nueva acerca de descargas del producto y comentarios de grupos de debate.

f) Pulse **Enviar**.

Resultados

Hasta que modifique las preferencias de **canal RSS** y **Mis notificaciones**, recibirá las notificaciones de las actualizaciones que ha solicitado. Puede modificar las preferencias cuando sea necesario (por ejemplo, si deja de utilizar un producto y empieza a utilizar otro).

Información relacionada

Canales de información RSS de soporte de software de IBM

Suscribirse a actualizaciones de contenido de soporte de Mis notificaciones

Mis notificaciones para soporte técnico de IBM

Visión general de Mis notificaciones para soporte técnico de IBM

Archivos de registro para solucionar problemas

IBM Data Risk Manager genera archivos de registro que puede utilizar para resolver problemas.

Puede utilizar los archivos de registro para comprobar el estado de los microservicios configurados con IBM Data Risk Manager.

Para obtener más información sobre las herramientas de diagnóstico, consulte “Herramientas de diagnóstico” en la página 203.

Visualización de los archivos de registro

1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
2. Pulse el icono de menú de aplicación  .
3. Pulse **Administración**.
4. En la página **Administración**, pulse **Diagnósticos**.
5. En la sección **Estado de la instancia** seleccione el microservicio para el que desea ver los archivos de registro.
6. Para ver el contenido del archivo de registro, pulse **Registros**.
7. Para descargar los archivos de registro, en **Descargar varios registros**, seleccione el archivo y, a continuación, pulse **Descargar**.
8. Revise los registros operativos.
9. Póngase en contacto con el soporte de IBM si se registran los mensajes de error.

Problemas de instalación del producto y métodos alternativos

Resuelva problemas que se pueden producir durante la instalación de IBM Data Risk Manager.

Los microservicios no se están ejecutando

Problema	Los microservicios no se ejecutan después de la instalación de IBM Data Risk Manager.

Causa	Uso incorrecto de nombre de host cuando se instala y se configura IBM Data Risk Manager.

Resolución	1. Conéctese al servidor de IBM Data Risk Manager a través de Secure Shell (SSH).
	SSH es un protocolo de red cifrado para conectarse de forma segura al servidor de IBM Data Risk Manager.
	2. Desde la línea de mandatos, ejecute el mandato siguiente para comprobar el estado de los microservicios configurados con IBM Data Risk Manager.
	`service dbscanner status`
	`service guardium status`
	`service idmanager status`
	`service listener status`
	`service symantec status`
	3. Ejecute los mandatos siguientes para iniciar los microservicios que no se están ejecutando. Asegúrese de que el servicio se ha detenido antes de iniciar el servicio.
	`service dbscanner start`
	`service guardium start`
	`service idmanager start`
	`service listener start`
	`service symantec start`

Problemas de configuración y método alternativo

Resuelva los problemas que pueden producirse al integrar IBM Security Guardium con IBM Data Risk Manager para importar los orígenes de datos.

Error de conexión durante la configuración de IBM Security Guardium

Problema	Es posible que encuentre problemas de conectividad al integrar IBM Security Guardium con IBM Data Risk Manager.
Causa	El error de conexión puede producirse por cualquiera de las razones siguientes: • Utilización de un URL incorrecto para conectarse a IBM Security Guardium. • Es posible que el microservicio de IBM Security Guardium no se esté ejecutando. • Se han proporcionado credenciales incorrectas para conectarse a IBM Security Guardium.

Resolución	**Especificación del URL correcto**
	1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`) como usuario `admin`.
	2. Pulse el icono de navegación de la aplicación  .
	3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
	4. En **Configuración de adaptador**, pulse **IBM Guardium**.
	5. En **Instancias de integración**, seleccione la instancia de IBM Security Guardium que necesita la corrección de URL.
	6. En **Detalles de instancia**, especifique el URL correcto en el campo **URL**.
	7. Pulse **Probar conexión** para probar si la comunicación entre la instancia de IBM Security Guardium e IBM Data Risk Manager es correcta.
	8. Pulse **Guardar**.
	Comprobación de si se está ejecutando el microservicio
	1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
	2. Pulse el icono de menú de aplicación  .
	3. Pulse **Administración**.
	4. En la página **Administración**, pulse **Diagnósticos**.
	5. Compruebe si el microservicio de IBM Security Guardium está en ejecución. Si el servicio se ha detenido, ejecute el mandato siguiente para comprobar el estado.
	a. Conéctese al servidor a través de SSH.
	b. En la línea de mandatos, ejecute el siguiente mandato.
	`service guardium status`
	6. Si el servicio se detiene, ejecute el mandato siguiente para iniciar el servicio.
	`service guardium start`
	Especificación de las credenciales correctas
	1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager.
	2. Pulse el icono de navegación de la aplicación  .
	3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
	4. En **Configuración de adaptador**, pulse **IBM Guardium**.
	5. En **Instancias de integración**, seleccione la instancia de IBM Security Guardium para la que se deben especificar las credenciales correctas.
	6. En **Detalles de instancia**, especifique el nombre de usuario y la contraseña correctos en los campos **Nombre de usuario** y **Contraseña**.
	7. Pulse **Guardar**.

Problemas de administración de usuarios y método alternativo

Resuelva problemas relacionados con el inicio de sesión de IBM Data Risk Manager y los permisos de usuario.

No se puede iniciar sesión en IBM Data Risk Manager

Término	Detalles
Problema	No se ha podido iniciar sesión en IBM Data Risk Manager con las credenciales especificadas.
Causa	El error de conexión puede producirse por cualquiera de las razones siguientes: • La cuenta de usuario está bloqueada. • La cuenta de usuario está deshabilitada. • La contraseña de la cuenta ha caducado.
Resolución	**Desbloqueo de una cuenta de usuario** 1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`) con privilegios de administrador. 2. Pulse el icono de navegación de la aplicación . 3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Usuario**. 4. En la lista **Usuarios de aplicación**, seleccione el nombre de usuario. 5. Deseleccione el recuadro de selección **Cuenta bloqueada**. 6. Pulse **Guardar**. **Habilitación de la cuenta de usuario** 1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Usuario**. 2. En la lista **Usuarios de aplicación**, seleccione el nombre de usuario. 3. Seleccione el recuadro de selección **Habilitar usuario**. 4. Pulse **Guardar**. **Cambio de contraseña** 1. Vaya a la página IBM Data Risk Manager**Iniciar sesión**. 2. Pulse la opción **Cambiar contraseña**. 3. Actualice la contraseña. 4. Haga clic en **Cambiar**.

No se puede acceder a las opciones de menú de IBM Data Risk Manager

Problema	Algunas de las opciones de menú de IBM Data Risk Manager no están disponibles.
Causa	Los permisos que están asociados a la cuenta de usuario limitan la navegación de la interfaz de usuario. Es posible que algunas de las opciones de menú no estén disponibles en función de los roles asignados.

Resolución	1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador. 2. Pulse el icono de navegación de la aplicación  . 3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Usuario**. 4. En la lista **Usuarios de aplicación**, seleccione el nombre de usuario que requiere acceso a las opciones de menú. 5. En la sección **Roles**, seleccione un rol. 6. Pulse **Guardar**.

Problemas de gestión de orígenes de datos y método alternativo

Resuelva los problemas que se producen al añadir orígenes de datos a IBM Data Risk Manager y descubrir orígenes de datos.

Problemas de conectividad al añadir orígenes de datos a IBM Data Risk Manager

Problema	Los orígenes de datos no se importan ni se guardan en IBM Data Risk Manager.
Causa	Es posible que se produzcan problemas de importación de origen de datos si especifica valores incorrectos para cualquiera de los siguientes parámetros de conexión de base de datos. • Credenciales de base de datos • Dirección IP o información de puerto • Nombre de la base de datos
Resolución	Asegúrese de que los parámetros de conexión de base de datos especificados son correctos. 1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`). 2. Pulse el icono de navegación de la aplicación  . 3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario**. 4. Seleccione **Origen de datos**. Se mostrará la lista de orígenes de datos. 5. Busque y localice el origen de datos. 6. En el origen de datos seleccionado, pulse el icono Acciones . 7. Para editar la información de conexión de base de datos, pulse el icono editar  . 8. Actualice la información de conexión de base de datos 9. Pulse **Añadir**.

No se puede ejecutar la operación de descubrimiento de origen de datos

Problema	El descubrimiento de orígenes de datos nativos no funciona. Cuando se ejecuta el descubrimiento nativo, la exploración está en estado En `cola`.
Causa	Es posible que Network Mapper (NMAP) no esté instalado en el servidor.

Resolución	Compruebe si NMAP está instalado en el servidor.
	1. Conéctese al servidor a través de SSH.
	2. Ejecute el mandato siguiente en una línea de mandatos para conocer la ubicación de NMAP.
	`whereis nmap`
	Si se ha instalado NMAP, la vía de acceso se muestra como `/usr/local/nmap`.
	3. Ejecute el mandato siguiente para conocer la versión de NMAP.
	`Nmap –version`
	4. Si no se devuelven resultados para los mandatos, póngase en contacto con el servicio de atención al cliente de IBM para resolver el problema.

Problemas de gestión de programas y método alternativo

Resuelva los problemas que se producen durante la creación y gestión de programas de IBM Data Risk Manager.

Los programas no son visibles en el panel de control

Problema	Los programas de IBM Data Risk Manager no son visibles en el panel de control.
Causa	El usuario no está autorizado para acceder a los programas.
Resolución	Asegúrese de que el usuario está asociado a un programa. 1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`) con privilegios de administrador. 2. Pulse el icono de navegación de la aplicación . 3. Pulse **Modelador de contexto empresarial**. En la página **Cartera de programas** se visualizará la lista de programas. 4. Seleccione el programa al que desea asociar un usuario y pulse el nombre del programa para editar el programa. 5. Pulse el icono **Ámbito**. 6. Seleccione el nombre de usuario. 7. Pulse **Asignar**.

El visualizador traza los datos de contexto empresarial incorrectamente

Problema	Los datos de contexto empresarial esperados no se pueden representar en el Visualizador de IBM Data Risk Manager. Por ejemplo, las aplicaciones dentro del ámbito de programa no se pueden trazar en el visualizador.
Causa	Es posible que los datos de contexto empresarial relevantes no se incluyan dentro del ámbito del programa.

Resolución	Asegúrese de que las entidades de contexto empresarial relevantes se añaden al ámbito de programa. 1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador. 2. Pulse el icono de navegación de la aplicación  . 3. Pulse **Modelador de contexto empresarial**. 4. Seleccione el programa en el que desea incluir datos de contexto empresarial y pulse el nombre del programa para editarlo. 5. Pulse el icono **Ámbito**. 6. En **Ámbito**, seleccione las entidades de contexto empresarial para LOB, `Aplicación`, `Plataforma`, `Conformidad`, `Entorno`, `Recurso` y `Origen de datos`. 7. Pulse **Asignar**.

El conjunto de selección de ámbito de programa no incluye todos los datos de contexto empresarial importados

Problema	No están disponibles todos los datos de contexto empresarial importados cuando se configura el ámbito de programa.
Causa	Los datos de contexto importados no tienen el conjunto de valores correlacionado correctamente.
Resolución	Revise los archivos CSV para los conjuntos de datos `Base de datos`, `Aplicación` y `Proceso empresarial` y compruebe si el conjunto de datos está correlacionado correctamente. Para obtener más información los datos de contexto empresarial, consulte “Correlación de datos de contexto empresarial” en la página 106.

Problemas de modelado de contexto empresarial y método alternativo

Resuelva los problemas que se producen al importar datos de contexto empresarial en el servidor de IBM Data Risk Manager.

No se han podido importar los datos de contexto

Problema	Se muestra el mensaje de error `Error de servidor interno` cuando se importan los datos de contexto.
Causa	• Es posible que los archivos CSV que se utilizan para importar los datos estén dañados. • Trabajos de importación incorrectos están bloqueando la operación de importación.

Resolución	**Comprobación de si los archivos CSV están dañados** 1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`). 2. Pulse el icono de navegación de la aplicación  . 3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**. 4. Pulse el icono de archivo CSV  para seleccionar los archivos CSV de `Base de datos`, `Aplicación` y `Proceso empresarial`. 5. Pulse **Cargar**. 6. Revise los archivos y valide la corrección de los datos. 7. Si los archivos CSV no están cargados en formato tabular, actualícelos. 8. Vuelva a cargar los archivos. **Comprobación de si los trabajos de importación están bloqueados** 1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`). 2. Pulse el icono de menú de aplicación  . 3. Pulse **Administración**. 4. Pulse la pestaña **Gestionar transacciones de carga**. 5. Identifique el tipo de transacción identificado como `IMPORT_WIZARD`. 6. Pulse **Eliminar transacción** para cancelar la operación de transacción. 7. Vuelva a cargar los datos de contexto.

No se pueden importar los datos de contexto debido a un conflicto de correlación

Problema	No se pueden importar los datos de contexto. En la vista previa, algunas columnas de la hoja de datos se muestran en rojo.
Causa	• Es posible que los archivos CSV que se utilizan para importar los datos estén dañados. • En las hojas de datos de contexto empresarial actualizadas que se cargan, es posible que los atributos de datos de contexto hayan cambiado.

Resolución	**Comprobación de si los archivos CSV están dañados** 1. Inicie sesión en IBM Data Risk Manager. 2. Pulse el icono de navegación de la aplicación . 3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**. 4. Seleccione los archivos CSV de `Base de datos`, `Aplicación` y `Proceso empresarial`. 5. Pulse **Cargar**. 6. Revise los archivos y valide la corrección de los datos. 7. Si los archivos CSV no están cargados en formato tabular, actualícelos. 8. Vuelva a cargar los archivos. **Eliminación de la transacción y carga de nuevo de los datos de contexto** 1. Inicie sesión en IBM Data Risk Manager Administration. 2. Pulse la pestaña **Gestionar transacciones de carga**. 3. Identifique el tipo de transacción identificado como `IMPORT_WIZARD`. 4. Pulse **Eliminar transacción** para cancelar la operación de transacción. 5. Vuelva a cargar los datos de contexto.

No se ha podido cargar el archivo CSV de datos de contexto

Problema	Cuando se carga el archivo CSV de datos de contexto, se visualiza el mensaje de error siguiente. `Formato de archivo no válido. Seleccione solo el formato de archivo CSV.`
Causa	Windows ha interpretado el tipo de archivo CSV como sin definir.

Resolución	1. Añada el contenido siguiente a un archivo de texto y guarde el archivo con un nombre `csv_import_config.txt`.
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.csv]`
	`"PerceivedType"="text"`
	`@="Excel.CSV"`
	`"Content Type"="text/csv"`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.csv\PersistentHandler]`
	`@="{5e941d80-bf96-11cd-b579-08002b30bfeb}"`
	2. Cambie el nombre de archivo por el nombre de `csv_import_config.reg`.
	3. Copie el archivo `csv_import_config.reg` en todos los sistemas donde está instalado IBM Data Risk Manager.
	4. Efectúe una doble pulsación en el archivo `csv_import_config.reg`.
	5. Pulse **Sí** para confirmar los cambios en los archivos de registro.
	El archivo de configuración añade el tipo de archivo como `text/csv`.
	6. Cargue los archivos CSV de datos de contexto que va a importar.

Problemas de importación de paquetes de solución y método alternativo

Resuelva los problemas que se producen al importar paquetes de solución en el servidor de IBM Data Risk Manager.

No se ha podido importar un paquete de solución

Problema	Se visualiza el siguiente mensaje de error cuando se importa el paquete de solución. `No se han podido guardar los datos`
Causa	• Es posible que los archivos CSV que se utilizan para importar el paquete de solución estén dañados. • Trabajos de importación incorrectos están bloqueando la operación de importación.
Resolución	**Comprobación de si los archivos CSV están dañados** 1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`). 2. Pulse el icono de navegación de la aplicación. 3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Paquete de solución**. 4. Pulse **Examinar** para seleccionar los archivos CSV para que se carguen el **Paquete de solución**, las **Políticas** y las **Tareas**. 5. Revise y valide la exactitud de los datos. 6. Actualice los archivos si es necesario. 7. Vuelva a cargar los archivos. **Comprobación de si los trabajos de importación están bloqueados** 1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`). 2. Pulse el icono de menú de aplicación. 3. Pulse **Administración**. 4. En la página **Administración**, pulse **Gestionar transacciones de carga**. 5. Identifique el tipo de transacción identificado como `IMPORT_WIZARD`. 6. Pulse **Eliminar transacción** para cancelar la operación de transacción. 7. Vuelva a cargar los datos de contexto.

La política de clasificador de IBM Security Guardium no se encuentra en la central de políticas

Problema	La política de clasificador de IBM Security Guardium que se ha importado como paquete de solución no está disponible en la **Central de gestión de políticas**.
Causa	La política no se ha desplegado en IBM Security Guardium.
Resolución	Despliegue de la política en IBM Security Guardium. 1. Vaya a **Modelador de contexto empresarial** > **Central de gestión de políticas**. 2. Busque la política que falta en **Descubrimiento y clasificación de datos**. 3. Una vez que se haya localizado la política, pulse **Desplegar**. 4. Seleccione **IBM Guardium** en la lista. 5. Pulse **Aceptar** para desplegar la política en IBM Security Guardium.

Problemas de gestión de políticas y método alternativo

Resuelva los problemas que se producen durante la creación y gestión de políticas.

Mensaje de error al importar políticas

Problema	Se produce un error al importar políticas de IBM Security Guardium.
Causa	• Trabajo de importación no satisfactorio. • Configuración incorrecta de IBM Security Guardium. • El microservicio de IBM Security Guardium no se está ejecutando.

Resolución	**Eliminación de la transacción y reimportación de políticas**
	1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
	2. Pulse el icono de menú de aplicación.
	3. Pulse **Administración**.
	4. En la página **Administración**, pulse **Gestionar transacciones de carga**.
	5. Identifique el tipo de transacción identificado como `POLICIES`.
	6. Pulse **Eliminar transacción** para cancelar la operación de transacción.
	7. Importe de nuevo las políticas.
	Verificación de la configuración de IBM Security Guardium
	1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**.
	2. Seleccione **IBM Guardium**.
	3. Revise los detalles de configuración y actualice según sea necesario.
	4. Para verificar la conectividad, pulse **Probar conexión**.
	5. Pulse **Guardar** después de la conexión satisfactoria a IBM Security Guardium.
	Verificación del estado de microservicios de IBM Security Guardium
	1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
	2. Pulse el icono de menú de aplicación.
	3. Pulse **Administración**.
	4. En la página **Administración**, pulse **Diagnósticos**.
	5. Compruebe si el microservicio de IBM Security Guardium está en ejecución. Ejecute el mandato siguiente para comprobar el estado.
	a. Conéctese al servidor a través de SSH.
	b. En la línea de mandatos, ejecute el siguiente mandato.
	`service guardium status`
	6. Si el servicio se detiene, ejecute el mandato siguiente para iniciar el servicio.
	`service guardium start`

Problemas de descubrimiento de datos y método alternativo

Resuelva los problemas producidos durante el descubrimiento de datos.

El origen de datos no se encuentra en el inventario

Problema	El origen de datos no se encuentra en el inventario de origen de datos y no está disponible para la exploración.
Causa	El origen de datos no está incluido en el ámbito del programa.
Resolución	Asegúrese de que el origen de datos se añade al ámbito del programa. 1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`) con privilegios de administrador. 2. Pulse el icono de navegación de la aplicación . 3. Pulse **Modelador de contexto empresarial**. En la página **Cartera de programas** se visualizará la lista de programas. 4. Seleccione el programa y pulse el nombre del programa para editar el programa. 5. Pulse el icono **Ámbito**. 6. En **Ámbito**, pulse el icono **Origen de datos**. 7. Seleccione los orígenes de datos. 8. Pulse **Asignar**.

La política de clasificador de IBM Security Guardium no se encuentra en el Centro de control y mandatos de seguridad

Problema	Las políticas de clasificador de IBM Security Guardium que se importan como paquete de solución no están disponibles en la Central de políticas para ejecutar la exploración.
Causa	No se ha desplegado la política en IBM Security Guardium.
Resolución	Asegúrese de que la política se despliega en IBM Security Guardium. 1. Vaya a **Modelador de contexto empresarial** > **Central de gestión de políticas**. 2. Busque la política que falta en **Descubrimiento y clasificación de datos**. 3. Una vez que se haya localizado la política, pulse **Desplegar**. 4. Seleccione **IBM Guardium** en la lista. 5. Pulse **Aceptar** para desplegar la política en IBM Security Guardium.

La exploración de clasificador de IBM Security Guardium ha fallado

Problema	La exploración de clasificador de IBM Security Guardium ha fallado.
Causa	• Credenciales del origen de datos incorrectas • Se ha suprimido el origen de datos en IBM Security Guardium • Se ha suprimido la política en IBM Security Guardium.

Resolución	**Verificación y corrección de la información de conexión de base de datos** 1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario**. 2. Seleccione **Origen de datos**. Se mostrará la lista de orígenes de datos. 3. Busque y localice el origen de datos. 4. Seleccione el origen de datos y pulse el icono Acciones ••• 5. Pulse el icono Editar  para actualizar la información de conexión de base de datos. 6. Pulse **Guardar**. **Creación de un origen de datos** 1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Origen de datos**. 2. Pulse el icono **Descargar** para resincronizar los orígenes de datos de IBM Security Guardium. 3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario**. 4. Pulse el icono **Añadir origen de datos** para crear un origen de datos. 5. Especifique toda la información necesaria. 6. Pulse **Guardar**. **Creación y despliegue de la política** 1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Políticas**. 2. Pulse el icono **Descargar** para resincronizar las políticas de clasificador de IBM Security Guardium. 3. Vaya a **Modelador de contexto empresarial** > **Central de gestión de políticas**. 4. Pulse el icono **Añadir política** para crear una política. 5. Especifique los detalles necesarios. 6. Pulse **Guardar**. 7. Despliegue la política en IBM Security Guardium.

IBM Security Guardium no se visualiza en el inventario

Problema	IBM Security Guardium no aparece listado en **Centro de control y mandatos de seguridad** > **Inventario** > **Infraestructura de datos**.
Causa	El dispositivo Guardium está incorrectamente configurado.
Resolución	Asegúrese de que IBM Security Guardium se ha configurado correctamente. 1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración**. 2. Seleccione **IBM Guardium**. 3. Revise los detalles de configuración y actualice según sea necesario. 4. Pulse **Probar conexión**. 5. Pulse **Guardar** después de la conexión satisfactoria a IBM Security Guardium.

Problemas de limpieza y análisis y método alternativo

Resolver problemas que se producen durante la limpieza y el análisis de datos.

No se dispone de un origen de datos explorado en el entorno de trabajo de análisis para la limpieza

Problema	El origen de datos explorado no se encuentra en el **Entorno de trabajo de análisis**.
Causa	El origen de datos ya está explorado y el conjunto de resultados se exporta al panel de control de IBM Data Risk Manager.
Resolución	Un comportamiento del sistema esperado.

La retrotracción de los niveles en el entorno de trabajo de análisis no funciona

Problema	Los intentos de retrotraer niveles en el **Entorno de trabajo de análisis** no funcionan.
Causa	No se admite la retrotracción de los niveles en el **Entorno de trabajo de análisis** después de que se exportan los activos.
Resolución	Ninguna

Problemas de publicación y correlación de taxonomías y métodos alternativos

Resuelva los problemas que se producen durante la correlación y la publicación de taxonomías de IBM Data Risk Manager.

Los valores de atributo de taxonomía predeterminados no están correlacionados

Problema	Para el activo seleccionado, los atributos de taxonomía no tienen ningún valor asignado de forma predeterminada.
Causa	Configuración y correlación de datos de contexto empresarial incorrectas.
Resolución	1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`) con privilegios de administrador. 2. Pulse el icono de navegación de la aplicación . 3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**. 4. Seleccione los archivos CSV de `Base de datos`, `Aplicación` y `Proceso empresarial`. 5. Pulse **Cargar**. 6. Pulse el icono Valores de configuración de la derecha. 7. Asegúrese de que el atributo **Aplicación** está configurado correctamente en la hoja `Aplicación`. 8. Pulse **Guardar**. 9. Pulse **Importar** para importar los datos de contexto con los cambios necesarios.

La página Taxonomía no muestra activos exportados

Problema	Después de la limpieza, el activo no se visualiza en la página **Centro de control y mandatos de seguridad** > **Taxonomía** > **Estructurados** > **Activos descubiertos recientemente**.
Causa	Configuración y correlación de datos de contexto empresarial incorrectas.
Resolución	1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**. 2. Seleccione los archivos CSV de `Base de datos`, `Aplicación` y `Proceso empresarial`. 3. Pulse **Cargar**. 4. Pulse el icono Valores de configuración de la derecha. 5. Asegúrese de que los atributos **Nombre de base de datos** y **Dirección IP** estén configurados correctamente en la hoja `Base de datos`. 6. Pulse **Guardar**. 7. Pulse **Importar** para volver a importar los datos de contexto.

Los valores de los campos Propietario de empresa y Guardián no se rellenan

Problema	Los campos **Propietario de empresa** y **Guardián** están vacíos para un activo recién descubierto.
Causa	Configuración y correlación de datos de contexto empresarial incorrectas.
Resolución	1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**. 2. Seleccione los archivos CSV de `Base de datos`, `Aplicación` y `Proceso empresarial`. 3. Pulse **Cargar**. 4. Pulse el icono Valores de configuración de la derecha. 5. Asegúrese de que los atributos **Nombre de base de datos** y **Dirección IP** estén configurados correctamente en la hoja `Base de datos`. 6. Pulse **Guardar**. 7. Pulse **Importar** para volver a importar los datos de contexto.

El activo de información no está disponible en los numerosos programas después de la exportación

Problema	Después de exportar el activo de información a varios programas, el activo no está disponible en dichos programas.
Causa	El origen de datos no se incluye en el ámbito del programa.

Resolución	Asegúrese de que el origen de datos está autorizado para el ámbito del programa. 1. Vaya a **Modelador de contexto empresarial**. 2. Seleccione el programa en el que desea incluir el origen de datos y pulse el nombre del programa para editarlo. 3. Pulse el icono **Ámbito**. 4. En **Ámbito**, pulse el icono **Origen de datos**. 5. Seleccione el origen de datos para el activo que no es visible e inclúyalo dentro del ámbito del programa. 6. Pulse **Asignar**.

Problemas de integración y método alternativo

Utilice la información de esta sección para solucionar los problemas que puedan surgir durante el proceso de instalación, desinstalación o migración de IBM Data Risk Manager.

Problemas de integración con Symantec DLP

La identificación de problemas se puede producir durante la integración de IBM Data Risk Manager con Symantec DLP.

Pestaña Sin estructurar no disponible en Taxonomía

Problema	No se puede ver la opción **Sin estructurar** en el módulo **Taxonomía**.
Causa	• El archivo JAR de incidencias no se ha cargado correctamente. • Symantec DLP no está configurado en el módulo **Configuración de adaptador integrado**.

Resolución	**Cargue el archivo JAR de incidencias** 1. Descargue el archivo JAR de incidencias en https://support.symantec.com/en_US/article.DOC9265.html. 2. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`). 3. Pulse el icono de navegación de la aplicación  . 4. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Políticas**. 5. Pulse el icono descargar  . 6. Seleccione la instancia de **DLP de Symantec**. 7. Pulse **Elegir archivo** para seleccionar y cargar el archivo JAR de incidencias de Symantec. **Configure Symantec DLP** 1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**. 2. Seleccione **Symantec DLP**. 3. Pulse el icono **Añadir instancia** para crear una instancia para DLP de Symantec. 4. Especifique los detalles necesarios. 5. Pulse **Guardar**.

Error de exploración de Symantec DLP

Problema	Aparece un mensaje de error al importar las exploraciones de Symantec DLP.
Causa	1. El archivo JAR de incidencias no se ha cargado correctamente. 2. URL incorrecto. 3. Configuración de ID de informe incorrecto.

Resolución	**Carga del archivo JAR de incidencias correcto** 1. Descargue el archivo JAR de incidencias en https://support.symantec.com/en_US/article.DOC9265.html. 2. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`). 3. Pulse el icono de navegación de la aplicación  . 4. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Políticas**. 5. Pulse el icono descargar  . 6. Seleccione la instancia de **DLP de Symantec**. 7. Pulse **Elegir archivo** para seleccionar y cargar el archivo JAR de incidencias de Symantec. **Verificación del URL** 1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**. 2. Seleccione **Symantec DLP**. 3. Compruebe si el URL especificado es correcto. **Verificación de los ID de informe** 1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Configuración de adaptador**. 2. Seleccione **Symantec DLP**. 3. Compruebe si los ID de informe especificados son correctos.

Error al importar un archivo CSV con incidencias

Problema	El mensaje de error se muestra cuando se importa un archivo CSV con incidencias.
Causa	• No se crea el destino en IBM Data Risk Manager. • Se ha especificado una vía de acceso de destino incorrecta. • El destino no está autorizado para un programa.

Resolución	**Cree un destino para Symantec DLP en IBM Data Risk Manager** 1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**. 2. Pulse **Almacenamiento de archivos**. 3. Pulse el icono **Añadir origen de datos**. 4. Especifique los detalles necesarios para la creación del destino. 5. Pulse **Añadir**. **Verifique la vía de acceso de destino** 1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Gestionar inventario** > **Origen de datos**. 2. Pulse **Almacenamiento de archivos**. 3. Seleccione el origen de datos y pulse el icono Editar. 4. Asegúrese de que la vía de acceso de **Vía de acceso de destino** es correcta. 5. Pulse **Guardar**. **El destino no está autorizado para el programa.** 1. Vaya a **Modelador de contexto empresarial**. 2. Seleccione el programa para el que debe estar autorizado el destino y pulse el nombre del programa para editarlo. 3. Pulse el icono **Ámbito**. 4. En **Ámbito**, pulse el icono **Origen de datos**. 5. Seleccione el origen de datos de destino. 6. Pulse **Asignar**.

Problemas de integración con IBM Security Guardium

La identificación de problemas se puede producir durante la integración de IBM Data Risk Manager con IBM Security Guardium.

Las opciones de selección de ámbito de VA están vacías cuando se desencadena la exploración

Problema	No se pueden ver los elementos de ámbito cuando se desencadena la exploración de vulnerabilidades.
Causa	No se han importado los datos de contexto.

Resolución	Importe los datos de contexto y añada la evaluación. 1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`). 2. Pulse el icono de navegación de la aplicación . 3. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Organización**. 4. Pulse el icono CSV para seleccionar las hojas `Base de datos`, `Aplicación` y `Proceso empresarial`. 5. Pulse **Cargar**. 6. Pulse el icono **Valores de configuración**. 7. Asegúrese de que las hojas `Base de datos`, `Aplicación` y `Proceso empresarial` están configuradas correctamente. 8. Pulse **Guardar**. 9. Pulse **Importar** para importar los datos de contexto con los cambios aplicados. 10. Vaya a **Gestión de vulnerabilidades**. 11. Pulse **Crear nueva evaluación**. 12. Pulse **Ámbito** para ver las entidades de la importación de los datos de contexto empresarial actualizada.

En el desencadenamiento de exploraciones de vulnerabilidades, las pruebas de VA se vuelven vacías

Problema	No se puede ver la lista de pruebas de VA cuando se inicia la exploración de VA.
Causa	Las pruebas de VA no se han importado de IBM Security Guardium.
Resolución	Importe las pruebas de VA de IBM Security Guardium. 1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Pruebas VA**. 2. Pulse el icono **Descargar** para descargar pruebas VA para todos los tipos de base de datos desde IBM Security Guardium.

La lista de dispositivos de IBM Security Guardium está vacía después de crearse el proceso de evaluación

Problema	La lista de dispositivos de IBM Security Guardium está vacía cuando se inicia el proceso de exploración.
Causa	El dispositivo IBM Security Guardium no está configurado para ejecutar VA.
Resolución	1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Integración** > **Integración** > **Configuración de adaptador**. 2. Seleccione **IBM Guardium**. 3. Seleccione la instancia en la lista. 4. Asegúrese de que **Ejecutar VA** esté seleccionado para los dispositivos de IBM Security Guardium en los que se van a desencadenar las exploraciones de VA.

Cuando se reparan las exploraciones de VA, la lista de actividades predefinida está vacía

Problema	La lista de actividades predefinidas está vacía cuando se crean elementos de acción para reparar las vulnerabilidades fallidas.
Causa	No se ha importado el paquete de solución.
Resolución	Asegúrese de que se importa el paquete de solución. 1. Vaya a **Modelador de contexto empresarial** > **Asistente de integración empresarial** > **Paquete de solución**. 2. Pulse **Examinar** en **Paquete de solución** para seleccionar los archivos CSV. 3. Pulse **Cargar**. Revise los archivos para ver si son correctos. 4. Pulse **Importar** para importar las políticas y las tareas en el servidor de IBM Data Risk Manager. 5. Vaya a **Gestión de vulnerabilidades** > **Vista de resultados**. 6. Seleccione las vulnerabilidades fallidas basándose en el nivel de gravedad **Crítico** y pulse **Reparar**. Se enumerarán las actividades predefinidas.

El valor de riesgo no se visualiza para los orígenes de datos en el panel de control de IBM Data Risk Manager

Problema	El valor de riesgo no se visualiza para los orígenes de datos en el widget **Infraestructura** del panel de control de IBM Data Risk Manager, incluso cuando los orígenes de datos tienen vulnerabilidades fallidas.
Causa	• La frecuencia de riesgo no se ha establecido. • El riesgo de infraestructura no se ha configurado.
Resolución	**Consulte la frecuencia de riesgo** 1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://`*`<dirección-IP-servidor-IDRM>`*`:8443/albatross/a3suite`). 2. Pulse el icono de menú de aplicación  . 3. Pulse **Administración**. 4. En la página **Administración**, pulse **Configuración del servidor** > **Valores de despliegue**. 5. Establezca la frecuencia de riesgo de acuerdo con los requisitos. 6. Pulse **Planificar**.

No se envían alertas de DAM desde IBM Security Guardium

Problema	No se envían alertas de DAM desde IBM Security Guardium.
Causa	• No se ha configurado el registro remoto en el dispositivo IBM Security Guardium. • La plantilla de mensaje de syslog no se ha definido correctamente en el dispositivo IBM Security Guardium.

Resolución	**Configuración del registro remoto en el dispositivo IBM Security Guardium**
	1. Configure SSH (Secure Shell) en el dispositivo IBM Security Guardium como el usuario `cli`.
	2. Verifique que el dispositivo esté configurado para tener el servidor de IBM Data Risk Manager como destino de registro especificando el mandato siguiente.
	`show remotelog`
	3. Si la salida del mandato devuelve una dirección IP y el puerto syslog del servidor de IBM Data Risk Manager, la configuración es correcta. De lo contrario, cree la entrada de registro remoto utilizando el mandato siguiente.
	`store remotelog add non_encrypted `all.all` <dirección_ip>:<puerto> tcp`
	Comprobación de la plantilla de mensaje
	Asegúrese de que la plantilla de mensaje de syslog se ha definido correctamente en el dispositivo IBM Security Guardium.

Las alertas de DAM no están etiquetadas a activos y orígenes de datos

Problema	Las alertas de DAM no están etiquetadas a los activos ni al infranodo en el panel de control.
Causa	• El microservicio de escucha de DAM no se está ejecutando. • El microservicio de escucha de DAM está registrando un mensaje de error.

Resolución	**Inicio del microservicio**
	1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
	2. Pulse el icono de menú de aplicación  .
	3. Pulse **Administración**.
	4. En la página **Administración**, pulse **Diagnósticos**.
	5. Compruebe si se ha detenido el microservicio de DAM. Ejecute el mandato siguiente para comprobar el estado.
	`service listener status`
	6. Si el servicio se detiene, ejecute el mandato siguiente para iniciar el servicio.
	`service listener start`
	Comprobación de los archivos de registro
	1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
	2. Pulse el icono de menú de aplicación  .
	3. Pulse **Administración**.
	4. En la página **Administración**, pulse **Diagnósticos**.
	5. Seleccione el microservicio **ESCUCHA DE DAM**.
	6. Pulse **Registros**.
	7. Pulse **Operativos**.
	8. Pulse **Descargar** en **Descargar varios registros**.
	9. Revise los registros operativos.
	10. Póngase en contacto con el soporte de IBM si se registran los mensajes de error.

No se ha creado la amenaza de DAM

Problema	No se ha creado la amenaza de DAM.
Causa	• El microservicio de escucha de DAM no se está ejecutando. • El microservicio de escucha de DAM está registrando mensajes de error. • La hora de aparición de la amenaza es incorrecta. • El trabajo cron no se está ejecutando.

Resolución	**Inicio del microservicio**
	1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
	2. Pulse el icono de menú de aplicación  .
	3. Pulse **Administración**.
	4. En la página **Administración**, pulse **Diagnósticos**.
	5. Compruebe si se ha detenido el microservicio de DAM. Ejecute el mandato siguiente para comprobar el estado.
	`service listener status`
	6. Si el servicio se detiene, ejecute el mandato siguiente para iniciar el servicio.
	`service listener start`
	Comprobación de los archivos de registro
	1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager con privilegios de administrador (`https://<dirección-IP-servidor-IDRM>:8443/albatross/a3suite`).
	2. Pulse el icono de menú de aplicación  .
	3. Pulse **Administración**.
	4. En la página **Administración**, pulse **Diagnósticos**.
	5. Seleccione el microservicio **ESCUCHA DE DAM**.
	6. Pulse **Registros**.
	7. Pulse **Operativos**.
	8. Pulse **Descargar** en **Descargar varios registros**.
	9. Revise los registros operativos.
	10. Póngase en contacto con el soporte de IBM si se registran los mensajes de error.
	Edición de la hora de aparición de amenazas
	1. Inicie sesión en la interfaz gráfica de usuario de IBM Data Risk Manager.
	2. Pulse el icono de navegación de la aplicación  .
	3. Vaya a **Modelador de contexto empresarial** > **Central de gestión de políticas**.
	4. Pulse el icono **Seleccionar tipo de política**.
	5. Seleccione **Supervisión de actividad de base de datos**.
	6. Seleccione la política para la que se ha definido la amenaza de DAM.
	7. En la sección Reglas de políticas y métricas, pulse el icono.
	8. Pulse el icono **Reparación** en la regla seleccionada.
	9. Para editar la información de configuración de amenazas, pulse el icono +.
	10. Edite la hora de aparición de la amenaza.
	11. Pulse el icono **Guardar**.
	Comprobación del estado de los trabajos cron
	1. Pulse **Diagnósticos** en la página **Administración**.
	2. Seleccione el microservicio **ESCUCHA DE DAM**.
	3. Pulse **Registros**.
	4. Pulse **Descargar** en **Descargar varios registros**.

Los riesgos asociados a amenazas de DAM no están correlacionados en el panel de control de IBM Data Risk Manager

Problema	No se está calculando el riesgo para la amenaza de DAM para el origen de datos asociado en el widget **Infraestructura** en el panel de control de IBM Data Risk Manager.
Causa	• La frecuencia de riesgo no se ha establecido. • El riesgo de infraestructura no se ha configurado.
Resolución	**Consulte la frecuencia de riesgo** 1. Inicie sesión en Suite de aplicaciones de IBM Data Risk Manager. 2. Pulse el icono de menú de aplicación . 3. Pulse **Administración**. 4. Pulse **Configuración de servidor** > **Valores de despliegue**. 5. Establezca la frecuencia de riesgo de acuerdo con los requisitos. 6. Pulse **Planificar**.

No se visualiza ningún mensaje de respuesta al ejecutar operaciones en IBM Data Risk Manager

Problema	No se visualiza ningún mensaje de respuesta cuando se ejecuta cualquier operación en IBM Data Risk Manager.
Causa	
Resolución	Es posible que el servidor de aplicaciones está inactivo. Póngase en contacto con el administrador del sistema.

Problemas de configuración de alta disponibilidad y método alternativo

Resuelva los problemas que se producen durante la configuración de alta disponibilidad de IBM Data Risk Manager.

No se pueden configurar las instancias de máquina virtual de IBM Data Risk Manager para alta disponibilidad

Problema	Problemas al configurar la alta disponibilidad de IBM Data Risk Manager.
Causa	Es posible que los servicios se hayan detenido en el nodo primario, el nodo BD o los nodos de aplicación.

Resolución	**Nodo primario**
	1. Inicie sesión en la instancia de máquina virtual (VM) de IBM Data Risk Manager como a3user a través de SSH.
	2. Compruebe el estado de los servicios siguientes que están configurados con IBM Data Risk Manager.
	Desde la línea de mandatos, ejecute los mandatos siguientes para comprobar el estado del servidor de equilibrio de carga y la base de datos maestra.
	`sudo service httpd status`
	`sudo service postgresql-10 status`
	Si los servicios se detienen, ejecute los mandatos siguientes para iniciar los servicios.
	`sudo service httpd start`
	`sudo service postgresql-10 start`
	Nodo BD
	1. Inicie sesión en la instancia de máquina virtual (VM) de IBM Data Risk Manager como a3user a través de SSH.
	2. Desde la línea de mandatos, ejecute el mandato siguiente para comprobar el estado de la base de datos esclava.
	`sudo service postgresql-10 status`
	Si el servicio de base de datos se detiene, ejecute el mandato siguiente para iniciar el servicio.
	`sudo service postgresql-10 start`
	Nodo de aplicación
	1. Inicie sesión en la instancia de máquina virtual (VM) de IBM Data Risk Manager como a3user a través de SSH.
	2. Desde la línea de mandatos, ejecute el mandato siguiente para comprobar el estado del servidor de aplicaciones.
	`sudo service tomcat status`
	Si el servicio se detiene, ejecute el mandato siguiente para iniciar el servidor.
	`sudo service tomcat start`
	3. Compruebe el estado de los microservicios siguientes que están configurados con IBM Data Risk Manager.
	Desde la línea de mandatos, ejecute los mandatos siguientes para comprobar el estado de los servicios.
	`sudo service appscan status`
	`sudo service dbscanner status`
	`sudo service guardium status`
	`sudo service idmanager status`
	`sudo service idrmintex status`
	`sudo service listener status`
	`sudo service symantec status`
	`sudo service igc status`
	`sudo service qradar status`
	`sudo service qradarva status`
	`sudo service servicenow status`
	`sudo service nativeus status`

Información legal

Contenido

Funciones de accesibilidad de IBM Data Risk Manager

Las funciones de accesibilidad ayudan a los usuarios con discapacidades, como por ejemplo movilidad restringida o visión limitada, a utilizar productos de tecnología de la información de manera satisfactoria.

Funciones de accesibilidad

La siguiente lista incluye las funciones de accesibilidad más importantes de IBM Data Risk Manager:

- Funcionamiento solo con el teclado
- Interfaces utilizadas normalmente por lectores de pantalla
- Teclas que son perceptibles al tacto, pero que no se activan por simple contacto
- Dispositivos estándar del sector para puertos y conectores
- La conexión de dispositivos alternativos de entrada y salida

Navegación mediante teclado

Este producto las teclas de navegación estándar de Microsoft Windows.

IBM y accesibilidad

Consulte el Centro de Capacidad y Accesibilidad Humana de IBM para obtener más información sobre el compromiso de IBM con la accesibilidad.

Declaración de copyright

Nota: Esta edición se aplica a la versión 2.0.6 de IBM Data Risk Manager (número de producto 5655-STP) y a todos los releases y las modificaciones posteriores, hasta que se indique lo contrario en nuevas ediciones.

Avisos

Esta información se ha desarrollado para productos y servicios que se ofrecen en los EE.UU. Es posible que IBM no ofrezca los productos, servicios o características descritos en este documento en otros países. Consulte al representante local de IBM para obtener información sobre los productos y servicios disponibles actualmente en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende indicar o implicar que sólo se pueda utilizar ese producto, programa o servicio de IBM. En su lugar puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no vulnere 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 patentes en tramitación que hagan referencia a temas tratados en esta publicación. La posesión de esta documentación no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Para realizar consultas sobre licencias relacionadas con la información del juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe sus 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 se aplica al Reino Unido ni a ningún otro país donde estas disposiciones sean incompatibles con la legislación vigente:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO PERO NO LIMITÁNDOSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO.

Algunas jurisdicciones no permiten la exclusión de garantías explícitas ni implícitas en determinadas transacciones, por lo que es posible que esta declaración no le concierna.

Es posible que esta publicación incluya inexactitudes técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar mejoras o cambios en los productos y/o programas descritos en esta publicación cuando lo considere oportuno y sin previo aviso.

Cualquier referencia incluida en esta información a sitios web que no sean de IBM sólo se proporciona para su comodidad y en ningún modo constituye una aprobación de dichos sitios web. El material de esos sitios web no forma parte del material de este producto de IBM y el uso de esos sitios web se hará bajo su responsabilidad.

IBM se reserva el derecho a utilizar o distribuir, en la forma que considere más adecuada, la información que se le facilite sin incurrir por ello en ninguna obligación hacia 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 independientemente y otros programas (incluido éste) y (ii) el uso mutuo de la información intercambiada, deberán ponerse en contacto con:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

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

El programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para él los proporciona IBM bajo los términos del Acuerdo de cliente de IBM, el Acuerdo de licencia de programa internacional de IBM o cualquier acuerdo equivalente entre ambas partes.

Todos los datos de rendimiento contenidos en este documento se han determinado en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Algunas mediciones se pueden haber realizado en sistemas experimentales y no

existe ninguna garantía de que estas mediciones sean las mismas en sistemas disponibles comercialmente. Además, es posible que algunas mediciones se hayan estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a 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 de disponibilidad pública. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni ninguna otra afirmación relacionada con productos que no son de IBM. Las preguntas sobre las posibilidades de los productos no IBM deben dirigirse a los proveedores de dichos productos.

Todas las declaraciones referentes a acciones e intenciones futuras de IBM pueden cambiar o ser retiradas sin aviso previo y solamente representan objetivos.

Todos los precios de IBM que se muestran son precios sugeridos por IBM para minoristas, están actualizados y se pueden modificar sin previo aviso. Los precios de los distribuidores pueden variar.

Esta información se proporciona solo con fines de planificación. La información contenida aquí puede cambiar antes de que los productos descritos pasen a estar disponibles.

Esta información cuenta con ejemplos de datos e informes que se utilizan en operaciones empresariales cotidianas. Para ilustrarlas de la forma más completa posible, los ejemplos incluyen los nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con nombres y direcciones utilizados por una empresa real es mera coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que ilustran técnicas de programación en las distintas plataformas operativas. Puede copiar, modificar y distribuir dichos programas de ejemplo bajo cualquier forma y sin tener que abonar una cuota a IBM, a fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación adaptados a la interfaz de programación de aplicaciones de la plataforma operativa para la que se han escrito los programas. Estos ejemplos no se han verificado exhaustivamente bajo todas las condiciones. Por lo tanto, IBM no puede garantizar ni implicar la fiabilidad, la capacidad de servicio ni el funcionamiento de estos programas. Los programas de ejemplo se proporcionan "TAL CUAL", sin garantía de ningún tipo. IBM no será responsable de ningún daño que surja del uso de los programas de ejemplo.

Cada copia o parte de estos programas de ejemplo o cualquier trabajo derivado debe incluir un aviso de copyright como el siguiente:

© (el nombre de la empresa) (año). Partes de este código se han obtenido de programas de ejemplo de IBM Corp. © Copyright IBM Corp. _especifique el año o los años.

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

Términos y condiciones de la documentación del producto

Los permisos para utilizar estas publicaciones se otorgan de acuerdo con los términos y condiciones siguientes.

Aplicabilidad
Estos términos y condiciones son adicionales a los términos de uso del sitio web de IBM.

Uso personal
Puede reproducir estas publicaciones para su uso personal, no comercial, siempre y cuando se conserven todos los avisos sobre propiedad. Queda prohibida la distribución, exposición o realizar trabajos derivados de estas publicaciones, o de cualquier parte de ellas, sin el consentimiento expreso de IBM.

Uso comercial
Puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de la empresa a condición de que se conserven todos los avisos de propiedad. No puede realizar trabajos derivados de estas publicaciones, ni reproducir, distribuir o mostrar estas publicaciones, ni parte alguna de las mismas, fuera de su empresa, sin el consentimiento expreso de IBM.

Derechos

Salvo si se indica lo contrario expresamente en este permiso, no se otorgan más permisos, licencias o derechos, expresos o implícitos, para las publicaciones o la información, datos, software y otras propiedades intelectuales contenidos en este documento.

IBM se reserva el derecho de anular los permisos otorgados aquí siempre que, a su discreción, considere la utilización de sus publicaciones perjudicial para sus intereses o, según lo determinado por IBM, considere que las anteriores instrucciones no se están siguiendo de forma adecuada.

No puede descargar, exportar ni reexportar esta información si no es cumpliendo totalmente todas las leyes y regulaciones aplicables, incluyendo las leyes y regulaciones de exportación de los Estados Unidos.

IBM NO GARANTIZA EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, YA SEAN EXPLÍCITAS O IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO INFRACCIÓN Y ADECUACIÓN A UN FIN DETERMINADO.

Marcas registradas

IBM, el logotipo de IBM, e ibm.com son marcas o marcas registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros nombres de productos y servicios podrían ser marcas comerciales de IBM u otras empresas. Encontrará una lista actualizada de las marcas registradas de IBM en http://www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript y todas las marcas registradas basadas en Adobe son marcas registradas o comerciales de Adobe Systems Incorporated en Estados Unidos y/o en otros países.

IT Infrastructure Library es una marca registrada de la Agencia central de informática y telecomunicaciones que ahora forma parte de la Oficina de Comercio del Gobierno.

Intel, el logotipo de Intel, Intel Inside, el logotipo de Intel Inside, Intel Centrino, el logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium y Pentium son marcas registradas o nombres comerciales de Intel Corporation o sus subsidiarias en los Estados Unidos y/o en otros países.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y/o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

ITIL es una marca registrada y una marca comunitaria registrada de la Cámara de Comercio, y está registrada en la Oficina de patentes y marcas de EE.UU.

UNIX es una marca comercial registrada de The Open Group en los Estados Unidos y otros países.

Java y todos los logotipos y marcas registradas basados en Java son marcas registradas de Oracle y/o sus filiales.

Cell Broadband Engine es una marca registrada de Sony Computer Entertainment, Inc en los Estados Unidos y/o en otros países y se utiliza bajo licencia.

Linear Tape-Open, LTO, el logotipo de LTO, Ultrium y el logotipo de Ultrium son marcas registradas de HP, IBM Corp. y Quantum en Estados Unidos y en otros países.

Declaración de procedimientos de seguridad recomendados

La seguridad de los sistemas de TI implica proteger los sistemas y la información mediante prevención, detección y respuesta a accesos indebidos desde dentro y 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 o sistema de las tecnologías de la información debería considerarse completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente efectivo para impedir la utilización o el acceso indebido. Los sistemas, productos y servicios de IBM están diseñados para formar parte de un método de seguridad completo, que deberá incluir procedimientos operativos adicionales y puede requerir otros sistemas, productos o servicios para contar con el máximo de efectividad. IBM NO GARANTIZA QUE LOS

SISTEMAS, PRODUCTOS O SERVICIOS SON INMUNES O HARÁN QUE SU EMPRESA SEA INMUNE A LA CONDUCTA MALINTENCIONADA O ILEGAL DE OTRA PARTE.

Índice

Caracteres Especiales

A

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W