IBM

Contents

IBM Data Risk Manager Quick Start Guide

Quick Start Guide

Version 2.0.6

This guide describes a quick and easy way to install and set up IBM Data Risk Manager.

Note:

About this task

Product overview

You can use IBM Data Risk Manager to discover, analyze, classify, monitor, and visualize business assets and risks that are associated with sensitive data. IBM Data Risk Manager provides the following capabilities:

- A programmatic process for ongoing discovery, classification, and reporting of sensitive data and associated risks across the enterprise.
- Automation assisted sustainable and efficient process to provide real-time business risk views.
- Association of assets with enterprise metadata such as business processes, applications, and stakeholders.

The IBM Data Risk Manager consists of various application modules such as Business Context Modeler (BCM), Security Command and Control Center (SC3) and the Data Risk Manager Dashboard.

Procedure

1. Access your software

   IBM Data Risk Manager is distributed as pre-configured software virtual appliance. The virtual appliance provides the entire software environment for Data Risk Manager installation that includes the hardened operating system. The image is in the Open Virtual Appliance (.ova) file format and is intended to be deployed to a virtual machine.

   You can download IBM Data Risk Manager, Version 2.0.6 from the IBM Passport Advantage website at http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm in the form of eAssembly packages for supported operating systems. For more information, see the "Software download instructions" section in the IBM Data Risk Manager documentation (https://www.ibm.com/support/knowledgecenter/SSJQ6V_2.0.6/com.ibm.idrm.doc/admin/top/cpt_admin_download.html).

   IBM Data Risk Manager package includes the following offerings:

   - Open Virtual Appliance (ova) image of the IBM Data Risk Manager
   - Product Quick Start Guide

   For complete documentation, including installation instructions, see the IBM Data Risk Manager documentation (https://www.ibm.com/support/knowledgecenter/SSJQ6V_2.0.6/com.ibm.idrm.doc/welcome.html).

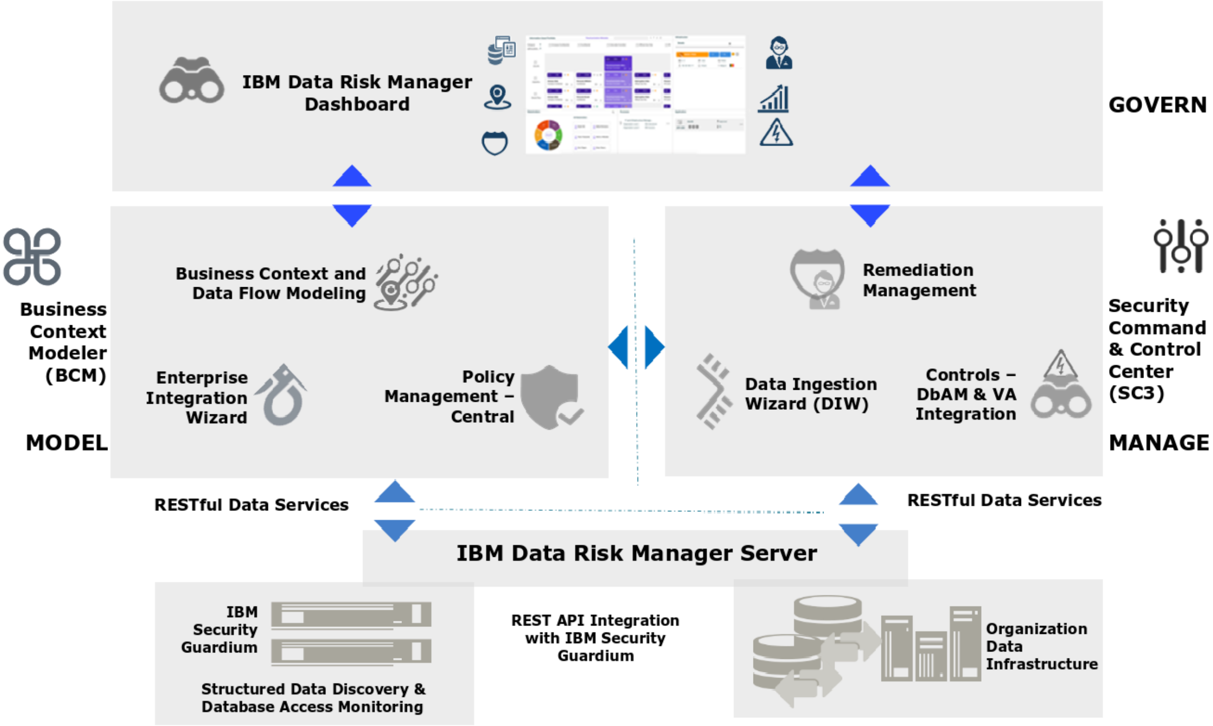
The IBM Data Risk Manager includes certain Red Hat software, which are subject to license agreements that can be viewed through: http://www-03.ibm.com/software/sla/sladb.nsf/displaylis/20E0A31663D6F996852581E500480032?OpenDocument

2. Evaluate your hardware and system configuration

   For information about system requirements and supported operating systems, see the "Installing and configuring" section of IBM Data Risk Manager documentation (https://www.ibm.com/support/knowledgecenter/SSJQ6V_2.0.6/com.ibm.idrm.doc/install/top/landing-install.html).

3. Review of the functional architecture

   Following functional architecture illustrates various modules and sub-modules of IBM Data Risk Manager. The functional modules of IBM Data Risk Manager are grouped to enable enterprises to model their enterprise context data with Business Context Modeler, manage via Security Command and Control Center and govern with IBM Data Risk Manager Dashboard.


IBM Data Risk Manager Dashboard
GOVERN
Business Context Modeler (BCM)
MODEL
Business Context and Data Flow Modeling
Enterprise Integration Wizard
Policy Management – Central
Remediation Management
Data Ingestion Wizard (DIW)
Controls – DbAM & VA Integration
Security Command & Control Center (SC3)
MANAGE
RESTful Data Services
RESTful Data Services
IBM Data Risk Manager Server
IBM Security Guardium
Structured Data Discovery & Database Access Monitoring
REST API Integration with IBM Security Guardium
Organization Data Infrastructure

4. Install IBM Data Risk Manager

   Planning your installation and importing virtual appliance.

   IBM Data Risk Manager virtual machine is by default thick-provisioned with 200 GB of storage. Based on your business requirements, you can modify the CPU utilization, memory, and hard disk capacity.

   For information about installation, see the "Installing and configuring" section of IBM Data Risk Manager documentation (https://www.ibm.com/support/knowledgecenter/SSJQ6V_2.0.6/com.ibm.idrm.doc/install/top/landing-install.html).

5. Configure

   Configuration of IBM Data Risk Manager is described in the "Installing and configuring" section of IBM Data Risk Manager documentation (https://www.ibm.com/support/knowledgecenter/SSJQ6V_2.0.6/com.ibm.idrm.doc/install/top/landing-install.html).

   For IBM Data Risk Manager troubleshooting information, see the "Troubleshooting and support" section in the documentation (https://www.ibm.com/support/knowledgecenter/SSJQ6V_2.0.6/com.ibm.idrm.doc/trouble/top/landing_trouble.html).

What to do next

More information

For more information, see IBM Data Risk Manager product support at http://www-947.ibm.com/support/entry/portal/overview/software/software_support_(general).

Software download instructions

You can obtain the downloadable installation images for IBM Data Risk Manager from the IBM Passport Advantage website.

Use the IBM Passport Advantage website at http://www-01.ibm.com/software/lotus/passportadvantage/pao_customer.html to purchase IBM Data Risk Manager. You can download or request a media pack of your entitled software.

The IBM Passport Advantage website provides packages, called eAssemblies, for IBM products.

The Fix Central website provides fixes and updates for software, hardware, and operating system of your system. IBM Data Risk Manager fix packs are published on the Fix Central website at http://www.ibm.com/support/fixcentral.

The “Installing and configuring” section on IBM Knowledge Center for IBM Data Risk Manager provides instructions for downloading, installing, and configuring IBM Data Risk Manager.

IBM Data Risk Manager installation images

IBM Data Risk Manager provides downloadable installation images.

Run the following steps to extract eImage packages:

1. Download the eImage package that you need. The eImage package is described in the following table.

   You can download the eImage package from the IBM Passport Advantage website at: http://www-01.ibm.com/software/lotus/passportadvantage/pao_customer.html
2. Unpack the eImage package into a temporary directory on your system.
3. Select a different temporary directory to use as a base directory for the installation.
4. Follow instructions in the “Installing and configuring” section on IBM Knowledge Center for IBM Data Risk Manager to install the product.

eImage	Description
CC4FREN	eImage for IBM Data Risk Manager, Version 2.6.

Product overview

The product overview contains topics that describe major concepts and other important information to help you use the system.

What's new in this release

Description of features and other information specific to the current release of IBM Data Risk Manager.

Integration exchange

IBM Data Risk Manager now supports the integration with following products.

IBM StoredIQ

You can integrate IBM Data Risk Manager with IBM StoredIQ to import unstructured data discovery inventory for risk analysis and actions. For more information about integration, see “Integrating IBM StoredIQ with IBM Data Risk Manager” on page 85.

ServiceNow

You can use IBM Data Risk Manager and ServiceNow integration to create, update, and, close ServiceNow incidents for remediation activities that are created in Action Center. For more information about integration, see “Integrating ServiceNow with IBM Data Risk Manager” on page 68.

Registry editor

In addition to uploading CSV files for context data mapping, you can also use the registry editor for mapping context data. You can use the Manage Inventory component to view and manage business context data. For more information about this new workflow, see “Managing inventory” on page 105.

Application residency view - Privacy Splash

The Geographic Distribution of Information Assets widget on IBM Data Risk Manager Privacy Splash page now shows application server locations on a global map. For more information about application residency view, see “Geographic Distribution of Information Assets” on page 161.

Action Center enhancements

You can now use IBM Data Risk Manager and ServiceNow integration to create, update, and, close ServiceNow incidents for remediation activities that are created in Action Center. Also, enhancements to Action Center for workflow management. For more information about Action Center, see “Action Center” on page 140.

Risk score evaluation

Various vectors are now used to automatically evaluate information asset risks. For more information about risk score evaluation, see “Risk modeling and visualization” on page 157.

IBM Data Risk Manager Dashboard enhancements

IBM Data Risk Manager Dashboard provides a broader view of data risks that are associated with an infrastructure of the information asset. For more information about the dashboard, see “IBM Data Risk Manager Dashboard” on page 164.

Assessment Outcome Management

Based on non-PRA assessment results, appropriate actions need to be implemented for addressing and mitigating the identified risks. You can use the Assessment Outcome Management module of IBM Data Risk Manager to view and manage risks. For more information about outcome management, see “Assessment Outcome Management” on page 186.

Exporting cleansed data sources to dashboard

You can directly export the cleansed IBM Security Guardium data sources to IBM Data Risk Manager Dashboard. For more information, see “Exporting cleansed IBM Security Guardium data sources to dashboard” on page 46.

IBM Data Risk Manager introduction

IBM Data Risk Manager provides business leaders a business-consumable data risk control center that helps to uncover, analyze, and visualize data-related business risks. Business leaders can then proactively address data-related business risks to protect their organizations.

IBM Data Risk Manager provides answers to the following questions about data risks.

- Which data is most critical?
- Where is the critical data located and are they protected?
- Who are the owners of critical data?

- Who is accessing the critical data?
- How the data is exposed to security risks?
- Who is accountable if the data is exposed?
- What are the appropriate steps to take based on the criticality of data?

Data protection challenges

Sensitive business information assets of an organization consist of customer information, intellectual property, employee information, merger and acquisition plans, financial information, sales strategy, and much more. These information assets are necessary and used by business processes across the organization that rely on their availability and integrity to complete their operations. In some cases, these information assets are the basis for competitive differentiation and provide a market advantage.

Gaining an understanding of the types of sensitive assets, their value to the organization, how they are protected, and what compliance requirements apply to the information are fundamental to make strategic decisions and apply appropriate controls.

This might seem like an overwhelming effort and many organizations might feel reluctant to undertake this journey. The organization might face the following challenges:

- Needing to discover sensitive information assets and yet unidentified data stores within a limited timeframe.
- Understanding sensitive data access, activity, and its flows to determine threats, exposures and vulnerabilities.
- Determining business risks that are associated with information assets and Identifying and prioritizing controls implementation.
- Demonstrating compliance with requirements from increasing regulatory and corporate mandates and internal audit.
- Reducing cost and complexity of deploying and managing monitoring solutions.

IBM Data Risk Manager provides enterprises with the following capabilities.

Uncover
Discovers databases and applications that contain crucial data of the organization.

Analyze
Provides insights into potential risks that might affect sensitive business information.

Visualize
Provides the executive team the visibility into their critical data.

Act
Creates sustainable, affordable, and ongoing processes to help manage critical assets and risks effectively.

Key features of IBM Data Risk Manager

Interactive data risk control center
Visualize and manage data in a unifying, single pane-of-glass view that helps convey value and meaning to business executives. Correlate security metrics from point security solutions to provide an end-to-end view of your security posture, by using the common language of risk to communicate with the C-suite and the risk office.

Data discovery and classification
Programmatically discover, classify, and report sensitive data and associated risks across the enterprise by integrating outputs from various software products. Uses real-time information to efficiently discover sensitive information assets and yet-unidentified data stores.

Automated analytics
Analyze identified risks, their type, affected information assets, and additional elements to deliver a comprehensive view of their potential probability and business impact. Based on the analytics, choose mitigating actions to help avoid suffering information losses.

Business risk evaluation and modeling

Correlate threats, vulnerabilities, controls, and business attributes with the value of the information asset. Calculate a risk score that highlights the parts of the business that are at risk.

Key benefits of using IBM Data Risk Manager

- Provides early visibility into potential risks that might affect sensitive business information assets and processes.
- Identifies specific and high-value business-sensitive information assets that are at risk due to internal or external threats.
- Provides a complete view of business metadata that is associated with sensitive data for the following items.
  - Applications
  - Processes
  - Policy and procedures
  - Controls and ownership
- Delivers value and meaning to business executives with a unique, easy-to-understand dashboard.
- Enables the right conversations with IT, Security, and line-of-business (LOB) teams to improve business processes and risks mitigation.
- Enables proactive measures to be taken to avoid potential impacts and avoid losses.

IBM Data Risk Manager components

IBM Data Risk Manager contains various components that work together to discover, analyze, classify, monitor, and visualize business assets and risks.

The IBM Data Risk Manager includes the following components.

IBM Data Risk Manager Dashboard

Delivers data visualization and management in a unifying, single pane of glass view that helps convey value and meaning to business executives. An interactive dashboard that enables information governance by providing visualization and management in a single, unifying console that depicts potential risks to sensitive business assets.

- Provides an interactive visualization of the information assets portfolio, data classification, and security requirements.
- Enables the application of proactive security controls and risk mitigation by providing visibility to potential risks, exposures, and vulnerabilities.
- Combines information assets, processes, and controls metadata to represent the data security and governance posture.
- Enables information governance by helping business leaders to visualize risks to sensitive assets across business functions and to understand potential organizational impacts.
- Provides compliance oversight through real-time notifications and action items in alignment with data security policies and requirements.

Business Context Modeler (BCM)

Models flow of data elements across the organization by collating entities and actors that include business process, applications, infrastructure nodes, and control specification.

- Defines discovery context by gathering and modeling information necessary for sensitive data discovery.
  - Infrastructure environment, such as network topology, application architecture, and data repositories.
  - Metadata information that is necessary to configure discovery infrastructure and scheduling of discovery scans.

- Discovery policies as they are relevant to respective discovery targets.

- Provides a visual representation of discovered data elements and its flow across organizational entities.
- Uses existing enterprise tools to gather information pertinent for discovery and data flow modeling.

Security Command and Control Center(SC3)

Provides a data-discovery-management solution that enables data discovery policy definitions, data discovery, analysis and cleansing of discovered data, information asset categorization, and remediation management.

- Defines discovery policies and classification rules to deploy on IBM Security Guardium and enables policy synchronization.
- Facilitates scan scheduling by using analysis and consolidation of inventory of discovery targets.
- Enables continuous delta discovery by automatically identifying changes in the inventory of discovery targets and schema.
- Repository of discovery and classification criteria, discovery and monitoring policies, threats, and vulnerabilities that are based on industry standards.
- Provides visibility to enterprise-critical information assets by grouping them against a preconfigured taxonomy based on classification criteria.

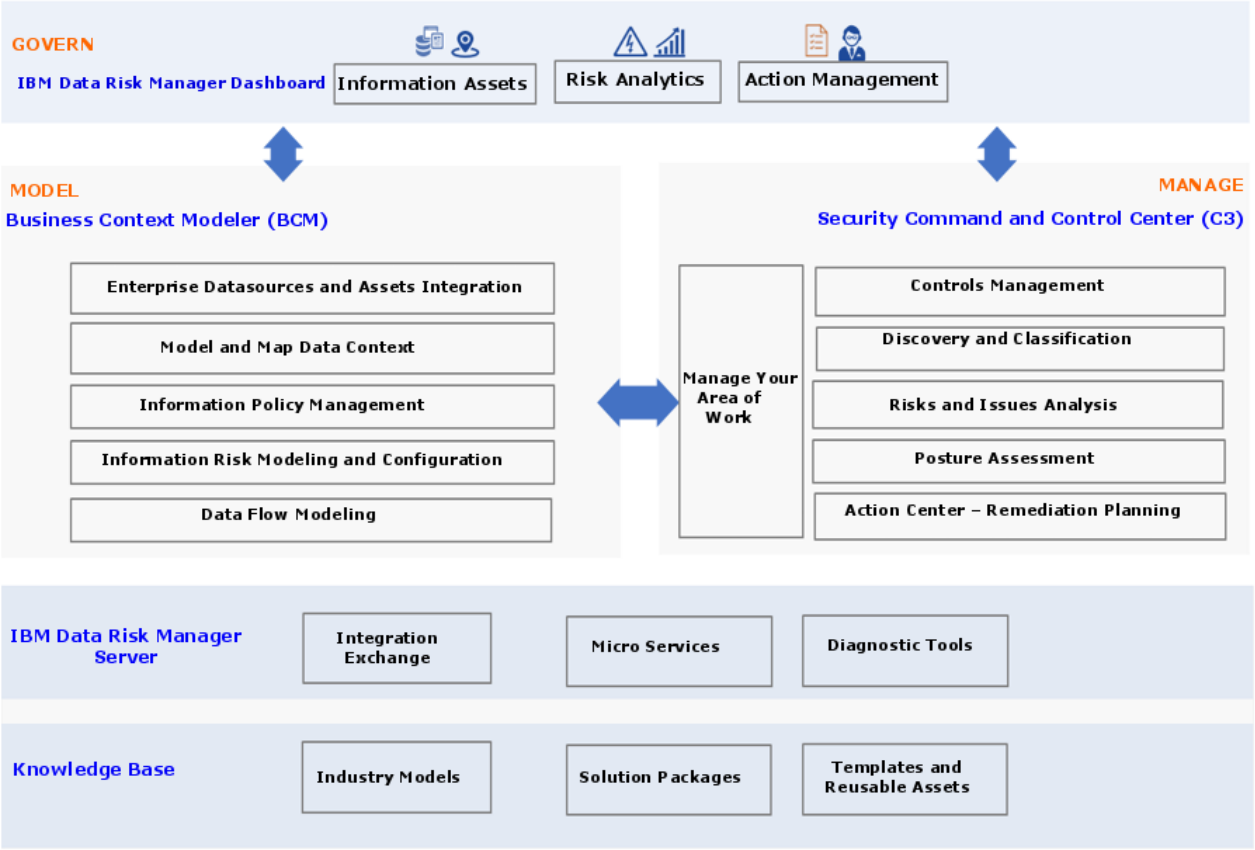
IBM Data Risk Manager Server

The server component of IBM Data Risk Manager.

IBM Data Risk Manager functional architecture

IBM Data Risk Manager architecture includes the Business Context Modeler (BCM), Security Command and Control Center (SC3), IBM Data Risk Manager Dashboard, and Data Risk Manager Application Server components to discover, analyze, classify, monitor, and visualize business assets and risks.

The following diagram illustrates IBM Data Risk Manager functional architecture.


GOVERN
IBM Data Risk Manager Dashboard
Information Assets
Risk Analytics
Action Management
MODEL
Business Context Modeler (BCM)
Enterprise Datasources and Assets Integration
Model and Map Data Context
Information Policy Management
Information Risk Modeling and Configuration
Data Flow Modeling
MANAGE
Security Command and Control Center (C3)
Manage Your Area of Work
Controls Management
Discovery and Classification
Risks and Issues Analysis
Posture Assessment
Action Center – Remediation Planning
IBM Data Risk Manager Server
Integration Exchange
Micro Services
Diagnostic Tools
Knowledge Base
Industry Models
Solution Packages
Templates and Reusable Assets

IBM Data Risk Manager architecture includes the following functional groups.

Model

Represents the functions that are associated with IBM Data Risk Manager setup, configuration, and alignment to the organizational context.

Data Flow Modeling

Enables the visual mapping of data assets flow within the organization across business and infrastructure entities.

Policy Management Central (PM Central)

Authors and manages IBM Data Risk Manager policies.

Enterprise Integration Wizard (EIW)

Includes all the functions that are related to integration with enterprise systems and import of repositories or other organization metadata. EIW functions include `User`, `User Group`, `Integration`, `Organization`, `A3 Repo`, `Native Discovery`, and `Manage Inventory`.

Framework Builder

The Model functional group includes the Business Context WebSphere Business Modeler component of IBM Data Risk Manager.

Manage

Represents the operational and day-to-day functions of IBM Data Risk Manager.

Data Ingestion Wizard (DIW)

Enables discovery, classifications, analysis, and taxonomy assignment of sensitive data of the organizations.

Remediation Management (Action Center)

Defines and manages product work flows that include action items, tasks, and stakeholder assignments. The work flows are used to manage data security programs, and to remediate issues and risks.

Controls - Database Activity Monitoring (DAM) and Vulnerability Assessment (VA)

Associated with integration of IBM Data Risk Manager with DAM and VA capabilities of IBM Security Guardium.

The Manage functional group includes the SC3 component of IBM Data Risk Manager.

Govern

Enables governance by providing visibility into the organizations data assets, sensitive asset types, and their value to the organization, how the data assets are protected, and what compliance requirements apply to the information for making strategic decisions. The Govern functional group includes the IBM Data Risk Manager Dashboard component.

Integration accelerators

IBM Data Risk Manager can be used with other security products to deliver an integrated solution.

IBM Data Risk Manager can be integrated with the following products that offers a programmatic process for ongoing discovery, classification and reporting of sensitive data, and associated risks across the enterprise.

- IBM Security Guardium
- IBM Security AppScan Enterprise
- Symantec DLP
- 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

Supported versions

Product	Version
IBM Security Guardium	10.5, 10.6, and 11.0
IBM Security AppScan Enterprise	9.0.3.8
Symantec DLP	12.x and 14.x
IBM QRadar Security Intelligence Platform	7.3.1
IBM InfoSphere Information Governance Catalog	11.5 and 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

Integration with IBM Security Guardium

Configure IBM Data Risk Manager to communicate with IBM Security Guardium to use its sensitive data-related risk information in IBM Data Risk Manager for risk analysis.

IBM Security Guardium is designed to help safeguard critical data. IBM Security Guardium helps ensure the integrity of information in data centers and automate compliance controls. For more information about IBM Security Guardium, see the product documentation at IBM Security Guardium documentation.

For more information about integration, see "Integrating IBM Security Guardium with IBM Data Risk Manager" on page 32.

Integration with IBM Security AppScan Enterprise

Configure IBM Data Risk Manager to communicate with IBM Security AppScan Enterprise for using its sensitive risk information in IBM Data Risk Manager for assessments.

IBM Security AppScan Enterprise enables organizations to mitigate application security risk, strengthen application security program management initiatives and achieve regulatory compliance. Security and development teams can collaborate, establish policies and scale testing throughout the application lifecycle. For more information about IBM Security AppScan Enterprise, see the product documentation at IBM Security AppScan Enterprise documentation.

For more information about integration, see "Integrating IBM Security AppScan Enterprise with IBM Data Risk Manager" on page 56.

Integration with Symantec DLP

Configure IBM Data Risk Manager to communicate with Symantec Data Loss Prevention connection (DLP) for importing Symantec DLP, Version 12.x and 14.x, incidents and policies into IBM Data Risk Manager.

Symantec Data Loss Prevention (Symantec DLP) is a content-aware security technology that helps companies understand where the sensitive corporate information is stored, how the data is being used, and how to protect data against loss and theft.

For more information about integration, see "Integrating Symantec DLP with IBM Data Risk Manager" on page 63.

Integration with IBM InfoSphere Information Governance Catalog
Configure IBM Data Risk Manager to communicate with IBM InfoSphere Information Governance Catalog for importing metadata into IBM Data Risk Manager.

IBM InfoSphere Information Governance Catalog is an interactive, web-based tool that enables users to create, manage, and share an enterprise vocabulary and classification system in a central catalog. IBM InfoSphere Information Governance Catalog helps users to understand the business meaning of their assets and provides search, browse, and query capabilities. For more information about IBM InfoSphere Information Governance Catalog, see the product documentation.

For more information about integration, see "Integrating IBM InfoSphere Information Governance Catalog with IBM Data Risk Manager" on page 70.

Integration with IBM QRadar Security Intelligence Platform
Configure IBM Data Risk Manager to communicate with IBM QRadar Security Intelligence Platform, Version 7.3.1, for using its sensitive data-related risk information in IBM Data Risk Manager.

IBM QRadar Security Intelligence Platform products provide a unified architecture for integrating security information and event management (SIEM), log management, anomaly detection, incident forensics, and configuration and vulnerability management. For more information about IBM QRadar Security Intelligence Platform, see the product documentation at IBM QRadar Security Intelligence Platform documentation.

For more information about integration, see Integrating IBM QRadar Security Intelligence Platform adapter.

Integration with ServiceNow
Configure IBM Data Risk Manager to connect and interact with ServiceNow for importing network topology data and taxonomy information into IBM Data Risk Manager.

For more information about integration, see "Integrating ServiceNow with IBM Data Risk Manager" on page 68.

Integration with Imperva SecureSphere
Configure IBM Data Risk Manager to connect and interact with Imperva SecureSphere for importing vulnerability information into IBM Data Risk Manager.

For more information about Imperva SecureSphere, see the product documentation.

For more information about integration, see "Integrating Imperva SecureSphere with IBM Data Risk Manager" on page 74.

Integration with IBM Multi-Cloud Data Encryption
Configure IBM Data Risk Manager to connect and interact with IBM Multi-Cloud Data Encryption to fetch encryption details of data sources that are added to the inventory from various sources where IBM Multi-Cloud Data Encryption agent is deployed for data encryption.

For more information about IBM Multi-Cloud Data Encryption, see the product documentation.

For more information about integration, see "Integrating IBM Multi-Cloud Data Encryption with IBM Data Risk Manager" on page 78.

Integration with OneTrust
Configure IBM Data Risk Manager to connect and interact with OneTrust to import inventories and their corresponding risk information into IBM Data Risk Manager. These risks are mapped to the appropriate information assets and infrastructure in IBM Data Risk Manager to view them on the dashboard for risk analysis and actions.

For more information about OneTrust, see the product documentation.

For more information about integration, see "Integrating OneTrust with IBM Data Risk Manager" on page 80.

Integration with IBM Security Guardium Analyzer

Configure IBM Data Risk Manager to connect and interact with IBM Security Guardium Analyzer for importing classifier scans and vulnerability information for risk analysis.

For more information about IBM Security Guardium Analyzer, see the product documentation.

For more information about integration, see "Integrating IBM Security Guardium Analyzer with IBM Data Risk Manager" on page 82.

Integration with IBM StoredIQ

Configure IBM Data Risk Manager to connect and interact with IBM StoredIQ to use its classification data results for risk analysis and actions.

For more information about IBM StoredIQ, see the product documentation at: https://www.ibm.com/support/knowledgecenter/SSSHEC_7.6.0/welcome/storediq.html

For more information about integration, see "Integrating IBM StoredIQ with IBM Data Risk Manager" on page 85.

User interface

IBM Data Risk Manager solution has a web-based application console (application suite) to manage various data discovery and classification functions, and to run various administrative tasks to set up and configure IBM Data Risk Manager environment.

Accessing IBM Data Risk Manager Application Suite

To access IBM Data Risk Manager Application Suite, type the following web address in your web browser:

```
https://<your-team-IDRM-Server-IPAddress>:8443/albatross/A3Suite/
```

<your-team-IDRM-Server-IPAddress> is the IP address of the server where IBM Data Risk Manager is installed.

License management

IBM Data Risk Manager generates IBM Software License Metric Tag (SLMT) files in a format that is supported by IBM License Metric Tool. IBM License Metric Tool then uses these files and generates License Consumption Reports.

Each instance of IBM Data Risk Manager generates SLMT (`.slmtag`) files. The monitored metric is `MANAGED_DEVICE`, and whose value is logged every time when an asset gets exported to IBM Data Risk Manager Dashboard.

The metric `MANAGED_DEVICE` is an infrastructure node that contains sensitive information assets. Total number of distinct infrastructure nodes that IBM Data Risk Manager manages is equal to the count in the value tag of the metric.

SLMT file format

The `.slmtag` files are stored in XML format with no root element for ease of modifications. The files consist of two parts:

- Header information, such as `SchemaVersion` and `SoftwareIdentity`.
- Periodically appended license consumption information (`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>
```

The `<Value>` tag indicates number of distinct infrastructure nodes that are exported to the dashboard at a time, which is specified by `<EndTime>`.

SLMT file configuration

The tag file is located under `/opt/ibm/slmtags` on the IBM Data Risk Manager server. When the `.slmtag` file size reaches the default 100 KB limit, log file rotation starts and the existing file is archived.

Supported languages

IBM Data Risk Manager supports various languages. The graphical (web) user interface labels, messages, and values can be displayed in both English language and in languages other than English.

IBM Data Risk Manager supports the following languages:

- English
- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese
- Spanish
- Traditional Chinese

Release information

The release information topics provide information that you need to know before you install and use the product, such its hardware and software requirements, and its known problems and limitations.

IBM Data Risk Manager known issues

Release notes contain information about IBM Data Risk Manager problems, limitations, and workarounds. Release notes are published as a technote.

You can access the technote at: https://www-01.ibm.com/support/docview.wss?uid=ibm11096012

System requirements

Your environment must meet the minimum system requirements to install IBM Data Risk Manager.

For more information about hardware and software requirements, see the *Installing and configuring* section on IBM Knowledge Center for IBM Data Risk Manager. The hardware and software requirements that are published are accurate at the time of publication.

Alternatively, see the detailed system requirements document at https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html.

1. Enter `IBM Data Risk Manager`.
2. Select the product version. For example, `2.0.6`.
3. Select the operating system.
4. Click **Submit**.

What's new in IBM Data Risk Manager, Version 2.0.4

Description of features and other information specific to version 2.0.4 of IBM Data Risk Manager.

IBM Data Risk Manager Reports

You can use IBM Data Risk Manager Reporting Engine for generating reports by using various predefined templates to easily view and analyze data. For more information about IBM Data Risk Manager reports, see "Reporting" on page 145.

IBM Data Risk Manager Scheduler

You can now use the IBM Data Risk Manager Scheduler function to create and manage jobs for automatically running various transactions at the intervals that you define. For more information about IBM Data Risk Manager Scheduler, see "IBM Data Risk Manager Scheduler" on page 151.

Integration servers

IBM Data Risk Manager now supports the integration with following products.

IBM Security Guardium Analyzer
For more information about integration, see "Integrating IBM Security Guardium Analyzer with IBM Data Risk Manager" on page 82.

IBM Multi-Cloud Data Encryption
For more information about integration, see "Integrating IBM Multi-Cloud Data Encryption with IBM Data Risk Manager" on page 78.

Privacy Splash

You can visualize data security and privacy information in various IBM Data Risk Manager Privacy Splash widgets in different ways that helps you to quickly analyze and address security and privacy risks. For more information about Privacy Splash, see "IBM Data Risk Manager Privacy Splash" on page 160.

Scope-based assessment and report

During assessment program creation for non-PRA-based frameworks, you can define scope of the assessment in terms of business entities or domains such as business processes, applications, and assets. Assessment scoping ensures that the necessary data is collected in effective and efficient manner for risk evaluation. For more information about assessment, see "Assessments" on page 175.

Enhancements to Questionnaire Builder - Decision tree

Responses to some questions lead to further questions. When creating a questionnaire, you can now express this relationship by creating a conditional relationship between questions and showing them in the form of a decision tree.

Enhancements to Security Command and Control Center dashboard

Improved Security Command and Control Center dashboard with more visualizations and enhanced usability that helps you to easily understand and interpret information. For more information about the dashboard, see "Security Command and Control Center dashboard" on page 129

IBM Data Risk Manager Dashboard Enhancements

- Revamp of Application widget to show data risks and privacy risks of the applications that are associated with the information assets.
- Revamp of dashboard secondary screen to view privacy risk information from OneTrust.

Data Modeler enhancements

Enhancements to Data Modeler component with new interface to make it easier for creating the diagrams.

Windows-based authentication for MSSQL server

For MSSQL server type, if the server is enabled to use Windows authentication, you can connect to the database by using Windows user login credentials for authentication.

LDAP authentication

IBM Data Risk Manager can be integrated with Lightweight Directory Access Protocol (LDAP) server to import user groups that are created in LDAP server.

What's new in IBM Data Risk Manager, Version 2.0.3

Description of features and other information specific to version 2.0.3 of IBM Data Risk Manager.

Business Context Modeling (BCM)

- Business context data import enhancements for all the integration sources.
- Program definition and provisioning including program BU hierarchy.
- Enhancement to Manage Inventory that now includes Server, Application, Database, and File Storage.
- Data Modeler enhancements with new interface.
- Allowing to update the location on the inventory.

Information Asset Dashboard

- Overlay IBM QRadar Security Intelligence Platform and IBM Security AppScan Enterprise scan vulnerability alerts on Infrastructure nodes.
- Splash page with configurable widgets and zoom feature on individual widgets.
- Splash – drill down for country-specific maps for data residency, policy violations, and vulnerabilities.
- Splash - policy violations and vulnerabilities pertaining to the top 10 Infrastructure.
- Integration of Infrastructure Map view on IBM Data Risk Manager Dashboard.
- Infrastructure risk enhancements.
- Configurability of dashboard widgets – colors and icons.
- Revamp of dashboard secondary screen with advance capability to view timeline based offenses and incidents from various sources.
- Category-based coloring

IBM QRadar Security Intelligence Platform integration

- Process alerts from IBM QRadar Security Intelligence Platform
- Overlay vulnerability alerts on Infrastructure (servers).
- Trigger vulnerability assessment scan on endpoints.
- Download endpoint vulnerabilities in BCM.

IBM Security AppScan Enterprise integration

- Enhancement to Vulnerability Assessment module and triggering scans.
- Download IBM Security AppScan Enterprise data in BCM.
- Overlay vulnerability alerts on application.

ServiceNow integration

- Context data enhancements for triggering data import.
- Import of business context from ServiceNow.
- Integration of Infrastructure Map view on IBM Data Risk Manager Dashboard.
- Support OAUTH based authentication for ServiceNow.

Imperva SecureSphere integration

Download of vulnerability scans from Imperva SecureSphere.

Server administration

- Admin Console Central Management tab provision to manage the agent restart activities, update password, distribute the patch (HA), unlock user, and view patch status.
- High Availability setup.
- Administration Console migration to IBM Data Risk Manager Application Suite.

Identity Management

- LDAP integration – import user groups.

Continuous functional enhancements

- Functional changes on Taxonomy module.
- Functional changes in IBM Data Risk Manager Dashboard – Information Asset secondary page.
- Functional changes on IBM Security Guardium Database Activity Monitoring.
- Risk engine enhancements.
- Taxonomy screen enhancements with asset tagging information.
- Row counts – locking tables on MSSQL database.

IBM InfoSphere Information Governance Catalog Integration

- Productize MVP2 of current version.
- Data import and mapping – Catalog and Context.
- Continuous notification (Kafka subscriber).
- De-componentization of IBM InfoSphere Information Governance Catalog.

Controls assessment

- Productizing Risk Assessment MVP (including enhancements).
- Functional enhancement identified based on MVP feedback on usability.
- Action Center integration.
- Qualitative assessment for asset ranking/evaluation.
- Support for multiple scoring models (condition and cumulative).
- Landing page for controls assessment.
- Generic Framework Assessment
- Option to upload CSV file for Questionnaires.

What's new in IBM Data Risk Manager, Version 2.0.2

Description of new features and other information specific to the current release of IBM Data Risk Manager.

IBM Data Risk Manager, version 2.0.2 provides the following capabilities:

Business Context Modeling (BCM)

- Business context data import enhancements for all the integration sources.
- Program definition and provisioning including program BU hierarchy.
- Enhancement to Manage Inventory that now includes Server, Application, Database, and File Storage.
- Data Modeler enhancements (UI simplification).

Information Asset Dashboard

- Overlay IBM QRadar Security Intelligence Platform and IBM Security AppScan Enterprise scan vulnerability alerts on Infrastructure nodes.
- Splash page with configurable widgets and zoom feature on individual widgets.
- Integration of Infrastructure Map view on IBM Data Risk Manager Dashboard.
- Infrastructure risk additions.

IBM QRadar Security Intelligence Platform integration

- Process alerts from IBM QRadar Security Intelligence Platform
- Overlay vulnerability alerts on Infrastructure (servers).
- Trigger vulnerability assessment scan on endpoints.
- Download endpoint vulnerabilities in BCM.

IBM Security AppScan Enterprise integration

- Enhancement to Vulnerability Assessment module and triggering scans.
- Download IBM Security AppScan Enterprise data in BCM.
- Overlay vulnerability alerts on application.

ServiceNow integration

- Context data enhancements for triggering data import.
- Import of business context from ServiceNow.
- Integration of Infrastructure Map view on IBM Data Risk Manager Dashboard.

Server administration

- Admin Console Central Management tab provision to manage the agent restart activities, update password, distribute the patch (HA), unlock user, and view patch status.
- High Availability setup.

Identity Management

- LDAP integration – import user groups.

Continuous functional enhancements

- Functional changes on Taxonomy module.
- Functional changes in IBM Data Risk Manager Dashboard – Information Asset secondary page.

- Functional changes on IBM Security Guardium Database Activity Monitoring.
- Risk engine enhancements.

IGC Integration

- Productize MVP2 of current version.
- Data import and mapping – Catalog and Context.
- Continuous notification (Kafka subscriber).

Installation images and fix packs

Obtain IBM Data Risk Manager installation files from the IBM® Passport Advantage® website and fix packs from Fix Central.

The Passport Advantage website provides packages, referred to as eAssemblies, for various IBM products at http://www-01.ibm.com/software/passportadvantage/pao_customer.html.

You can use Fix Central to find the fixes that are provided by IBM Support for various products, including IBM Data Risk Manager at https://www-945.ibm.com/support/fixcentral. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options.

Installing and configuring

Installing is an activity in which you put software onto systems.

The installation topics provides information about prerequisite software and hardware, and also installing the product.

The configuring topics are geared towards your initial configuration and customization of the product.

Installation overview

Install IBM Data Risk Manager in a virtual environment by using the VMware platform. IBM Data Risk Manager is provided as a VMware virtual application in Open Virtual Appliance (OVA) format.

IBM Data Risk Manager is deployed as an on-premises solution, developed as a web application based on client/server architecture model. You can configure the application to support various non-functional requirements such as high-availability and disaster recovery management.

Installation prerequisites

Before you install and deploy IBM Data Risk Manager, understand the prerequisites and plan your environment.

Hardware specifications for a stand-alone server virtual machine (VM)

Processor	5 GHz or higher
Number of processors	4
Memory (RAM)	16 GB
Network	Dual 1 Gbps
Storage	200 GB
Architecture	64-bit

Software specifications to deploy IBM Data Risk Manager virtual image (OVA file)

Operating system	VM host – VMware ESXi 5.5 or later
Connectivity	100 Mbps LAN
Deployment and maintenance	Server can be accessible over intranet (through VPN) for installation and configuration.

Client specifications for desktops, notebooks, or workstations

CPU	2.33 GHz (x86 compatible)
Memory (RAM)	4 GB
Operating system	Microsoft Windows 10 / Mac OSX
Browser	Chrome 59 or later and Firefox 52 or later

Supported databases

Database	Version
MySQL	5.7.19+
Oracle	11g and 12c
SQL Server	Server 2012 and Server 2016
Sybase	16.0
IBM Db2	11.1
Postgres	9.6+

Integration accelerators

IBM Data Risk Manager can be integrated with the following products that offers a programmatic process for ongoing discovery, classification and reporting of sensitive data, and associated risks across the enterprise.

Product	Version
IBM Security Guardium	10.5.0, 10.6.0, and 11.0
IBM Security AppScan Enterprise	9.0.3.8
Symantec DLP	12.x and 14.x
IBM QRadar Security Intelligence Platform	7.3.1
IBM InfoSphere Information Governance Catalog	11.5 and 11.7
Imperva SecureSphere	13.0.0.10
ServiceNow	Kingston
OneTrust	NA
IBM Multi-Cloud Data Encryption	2.2
IBM Security Guardium Analyzer	NA
IBM StoredIQ	7.6.0.17

Network configuration settings

Port/Protocol	Service	Source	Destination
22/TCP	**ssh** Command-line access to administer and manage IBM Data Risk Manager Server.	Remote desktop	IBM Data Risk Manager Server
9003/TCP	**Syslog** Receives syslog notifications from the IBM Security Guardium appliance.	IBM Security Guardium appliance (if installed)	IBM Data Risk Manager Server
9000/TCP	**Syslog** Receives syslog notifications from the IBM QRadar Security Intelligence Platform appliance.	IBM QRadar Security Intelligence Platformappliance (if installed)	IBM Data Risk Manager Server
8009 /TCP	**AJP** For IBM Data Risk Manager High Availability (HA).	IBM Data Risk Manager HA server	IBM Data Risk Manager Server
8443/TCP	**https** IBM Data Risk Manager server connectivity to IBM Data Risk Manager client applications.	Bi-directional communication between IBM Data Risk Manager client applications and IBM Data Risk Manager Server	Supported web browsers
8762/TCP	Native database scanner	IBM Data Risk Manager Server	Target systems where database servers are hosted. For example, Oracle, MySQL, or SQL Server.
8764/TCP	Symantec DLP agent	IBM Data Risk Manager Server	Symantec DLP appliance
8765/TCP	Security Identity Manager agent	Bi-directional communication between Security Identity Manager agent and LDAP Server/SSO server	LDAP server port need to be open either at 389 (LDAP) or 636 (LDAP and SSO server)
8766/TCP	Unstructured scanner	IBM Data Risk Manager Server	Target remote file share system where SMB or SFTP are enabled.
8768/TCP	IBM InfoSphere Information Governance Catalog scanner	IBM Data Risk Manager Server	IBM InfoSphere Information Governance Catalog appliance
8787/TCP	ServiceNow agent	IBM Data Risk Manager Server	Service Now appliance
2529/TCP	IBM Data Risk Manager management agent	IBM Data Risk Manager Server	IBM Data Risk Manager Server

Deployment checklist

- Choose the location to place IBM Data Risk Manager Server VM.
- Document the IP address and host name for assigning to the IBM Data Risk Manager Server VM.
- Ensure that IBM Data Risk Manager Server and the database servers are connected.
- Decide on the products and applications to integrate with IBM Data Risk Manager and ensure its availability and access.
- Creation of service account on the integration products and databases that are in scope with necessary privileges to run metadata scans.

Deploying IBM Data Risk Manager virtual image

To install IBM Data Risk Manager in a VMware environment, deploy the appliance OVA template. Deploying an OVA template creates a virtual appliance that contains the application on a VMware host such as an ESXi server.

Before you begin

- Download and extract the OVA package IBM Data Risk Manager to a directory. The file is available for download from the IBM Passport Advantage website. See the "Software download instructions" on page 3 topic for details.
- Review the Installation prerequisites topic to know the prerequisite information for installing and configuring IBM Data Risk Manager.

Procedure

1. Download the IBM Data Risk Manager OVA template installation file from Passport Advantage Online.
2. Open the VMware vSphere client.
3. Select **File** > **Deploy OVF Template**.
4. Click **Browse** to locate the OVA file that you downloaded and select the file.
5. Click **Next**.
6. Provide a meaningful name for the template, which becomes the name of your virtual machine. Identify an appropriate location to deploy the virtual machine. Click **Next**.
7. Select **Thick Provision Lazy Zeroed** as the disk format to store the virtual disks. It is recommended that you select thick provisioning, which is preselected for optimized performance. Click **Next**.
8. Map networks for the deployed template to use. Click **Destination Networks** to view the available networks on the ESX server. Select a destination network to define the appropriate IP address allocation for the virtual machine deployment. Click **Next**.
9. Review your deployment settings. If you want the server to start as soon as it is deployed, select **Power on after deployment**.
10. Click **Finish** to close the Deploy OVF Template wizard and deploy the virtual machine. Deploying the virtual machine might take several minutes.

What to do next

Define your IBM Data Risk Manager configuration by using the command-line interface of IBM Data Risk Manager Server. For more information, see Configuring IBM Data Risk Manager Server.

Use the VMware vSphere client to configure virtual appliance hardware options for the IBM Data Risk Manager virtual appliance. For more information, see Upgrading hard disk and Upgrading RAM.

Configuring IBM Data Risk Manager Server

After IBM Data Risk Manager virtual appliance is deployed in the VMware environment, you must complete a few configuration tasks.

Before you begin

Ensure that the IBM Data Risk Manager virtual image is successfully deployed in a VMware environment. For information about how to deploy the virtual image, see "Deploying IBM Data Risk Manager virtual image" on page 20.

About this task

After IBM Data Risk Manager appliance is deployed on a virtual network, you must complete the initial configuration by using the command-line interface of the server.

Procedure

1. Log on to the IBM Data Risk Manager virtual machine by using the default user name and password.

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

   After the first login, the a3user can run the **`passwd`** command to change the default password.
2. Assign the IP address to Server.

   IBM Data Risk Manager

   a. Run the following command to view active network (Ethernet) interfaces in the virtual machine, which is in the format `ifcfg`-XX.

   ```
   # ip a
   ```

   Sample output for the command `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
   ```

   In this sample, `ens33` represents the value of XX in the `ifcfg`-XX format.

   b. In the output of the command, value of XX in the `ifcfg`-XX format is other than `ens33`, for example, `ens66` or `eth0`, run the following step.

   Go to the following directory and check whether the `ifcfg`-XX file exists.

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

   If the `ifcfg`-XX file exists, go to step c. Else, run the following command.

   ```

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

   c. Run the following command to locate and open the interface configuration file for editing.

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

   d. Edit following properties in the interface configuration file. Keep the default values for the remaining properties.

BOOTPROTO	`dhcp` Or `static`
NAME	XX, for example ens33
DEVICE	XX, for example ens33
IPADDR	IP address that is assigned to IBM Data Risk Manager, for example, 9.195.17.227.
PREFIX	The subnet mask, for example, 23.
NETMASK	Default network subnet mask address, for example, 255.255.254.0.
GATEWAY	Default network gateway IP address, for example 9.195.16.1.
DNS1	Address of the Domain Name Server (DNS), for example, 9.0.146.50.
DNS2	DNS address, for example, 9.0.148.50.

The following example shows file contents.

```
[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. (Optional) Configure the DNS server.

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

f. Restart the network service.

```
# sudo service network restart
```

g. For VHD format, you must run the following command.

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

h. To get the actual IP address for OVA and VHD formats, run the following command.

```
ip a
```

3. Assign the host name or add `datariskmanager-server.ibm.com` in the network DHCP list.

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

4. Assign date, time, and time zone to the IBM Data Risk Manager Server.

a. Set the date and time for IBM Data Risk Manager Server.

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

Ensure that time zone of the NTP server is correct.

b. Run the following command to verify the date and time.

```
# date
```

c. Run the following command to ensure that the hardware clock is in sync with the system date and time.

```
sudo hwclock --systohc
```

d. Run the following command to verify whether the hardware clock date and time is updated.

```
sudo hwclock
```

e. Update the time zone.

1)

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

2) Run the following command to verify whether the time zone is correctly updated.

```
 # date
```

f. If the time zone is updated, delete the old file and restart the server.

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

What to do next

Verify whether you can access IBM Data Risk Manager Application Suite.

1. Open IBM Data Risk Manager Application Suite by using the following URL.

```
https://<IDRM-Server-IP-Address>:8443/albatross/a3suite
```

2. Specify the following user name and password.

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

3. Change the password when prompted.
4. Accept the license agreement.
5. Register the IP address in IBM Data Risk Manager Admin Console.

   a. Log on to IBM Data Risk Manager Admin Console (`https://<IDRM-Server-IP-Address>:8443/albatross/index`) as `admin` user.

   b. Click **Central Management**.

   c. Click **Register**.

   d. Specify the IP address in **Host IP Address**.

   e. If SSH password of `a3user` is changed, specify the SSH password in **Host SSH Password**.

   f. Click **Register**.

   g. Click **Update Password**.

   h. Specify the updated password in **Update Password**.

   i. Click **Update**.

Increasing virtual memory

You might need to increase the virtual memory for a better performance of IBM Data Risk Manager.

Before you begin

The virtual machine that you are configuring must be powered off.

About this task

Increase the memory size from 16 GB to 32 GB in the virtual machine.

Procedure

1. Click **Virtual Machine** > **Settings**.
2. In the Memory section, set the amount of memory to allocate to the virtual machine by using the **Memory** slider control.
3. Save the settings.
4. Start the virtual machine.

What to do next

Verify the memory settings.

1. Log on to IBM Data Risk Manager virtual appliance by using the default user name and password.
2. In the command-line interface, run the following command to display size of the memory in GB.

```
free -g
```

Increasing virtual hard disk size

If the preconfigured disk space is not sufficient, you can increase the virtual disk size for IBM Data Risk Manager.

Before you begin

The virtual machine that you are configuring must be powered off.

About this task

Increase the hard disk size from 200 GB to 300 GB in the virtual machine. After the virtual disk size is increased, you need to increase the hard disk partition. The partitioning tool `GParted` can be used for partitioning.

Procedure

1. Click **Virtual Machine** > **Settings**.
2. Select the IBM Data Risk Manager virtual machine disk, for example, `idna-server-disk.vmdk`.
3. Use the **Disk size** slider to set the new size.
4. To resize the virtual hard disk, click **Apply**.
5. Click **OK**.
6. Connect the CD.
7. Assign the CD drive to the `GParted` ISO file.
8. Select the option **CD/DVD** to start the virtual machine. Click **Restart** to start the GParted partitioning tool.
9. For a default keyboard, select the option **Don't touch key map**.
10. Select language by typing the number against your preferred language and press enter. Default is US English.

11. Select display mode by typing the number against your preferred mode and press enter.

    The "**/dev/sda - GParted**" page is displayed.
12. Click **Partition** > **Resize/Move**.
13. On the "**Resize/Move /dev/sda1**" page, specify the following values.

Option	Description
Free space preceding (MiB)	0
New size (MiB)	255999
Free space following (MiB)	0
Align to	MiB

14. Click **Resize/Move**.
15. Click **Apply**.
16. Click **Close** when the action completes successfully.
17. Click **Exit**.
18. To restart the virtual machine, select **Reboot**.

What to do next

Verify the hard disk size.

1. Log on to IBM Data Risk Manager virtual appliance by using the default user name and password.
2. In the command line interface, run the following command to display the hard disk size.

```
df -h
```

Setting up high availability in IBM Data Risk Manager

To help maintain continuous IBM Data Risk Manager operations, you can set up your environment for high availability.

Configuring high availability

Enabling IBM Data Risk Manager high availability function in an integrated infrastructure environment minimizes system downtime and provides disaster recovery capabilities.

Terminologies used in high availability setup

Primary Node

Primary Node VM instance is used by the client to access IBM Data Risk Manager. IBM Data Risk Manager Load Balancing Server and Master Database runs on the Primary Node.

DB Node

IBM Data Risk Manager Slave Database runs on the DB Node VM instance.

Application Node

Services that are necessary to run IBM Data Risk Manager must be running on all the Application Node VM instances.

Master Database

Database on the Primary Node VM instance is the Master Database. Read and write operations can be performed on the Master Database.

Slave Database

Database on the DB Node VM instance is the Slave Database. Only the write operation can be performed on Slave Database.

Requirements and considerations for high availability configuration

- Currently, for IBM Data Risk Manager high availability, you can configure one Primary Node, one DB Node, and a maximum of two Application Nodes.
- Primary Node must always be running to access Application Node.
- If one of the IBM Data Risk Manager Application Nodes is down, the other Application Node can continue to serve the requests.
- If IBM Data Risk Manager DB Node is down, you can continue to use the IBM Data Risk Manager system. When the DB Node is up and running, the captured delta data is replicated automatically to the DB Node (Slave).
- Ensure that Application Nodes must have a minimum of 16-GB RAM.
- During the configuration process, you can exit any time if necessary. However, after the configuration process is complete on an IBM Data Risk Manager VM instance, it cannot be reverted. You must reinstall the VM instance and start the configuration process again.
- If an IBM Data Risk Manager VM instance is already configured as Primary Node, DB Node, or Application Node, further configuration is not allowed.

High availability configuration process

To set up a high availability environment in IBM Data Risk Manager, complete the following steps.

1. Install, for example,IBM Data Risk Manager on four virtual machine instances. For installation steps, see "Deploying IBM Data Risk Manager virtual image" on page 20.
2. Determine which of the VMs act as Primary Node, DB Node, or Application Node.
3. Configure the Primary Node VM. For the configuration steps, see "Configuring Primary Node" on page 28.
4. Configure the DB Node VM. For the configuration steps, see "Configuring DB Node" on page 28.
5. Configure the Application Node VMs. For the configuration steps, see "Configuring Application Nodes" on page 29.
6. After configuration of all the VM instances for high availability, you can access IBM Data Risk Manager by using the following web address.

   ```
   https://PRIMARY_NODE_IP_ADDRESS:8443/albatross/A3Suite
   ```

7. You can view the IBM Data Risk Manager high availability status at the following location.

   ```
   https://PRIMARY_NODE_IP_ADDRESS:80/status
   ```

Troubleshooting high availability configuration problems and workaround

Log files are generated when the IBM Data Risk Manager VM instances are configured for high availability that support team can use to troubleshoot problems. The log files are stored at `~/agile3/HA_Configure.log`.

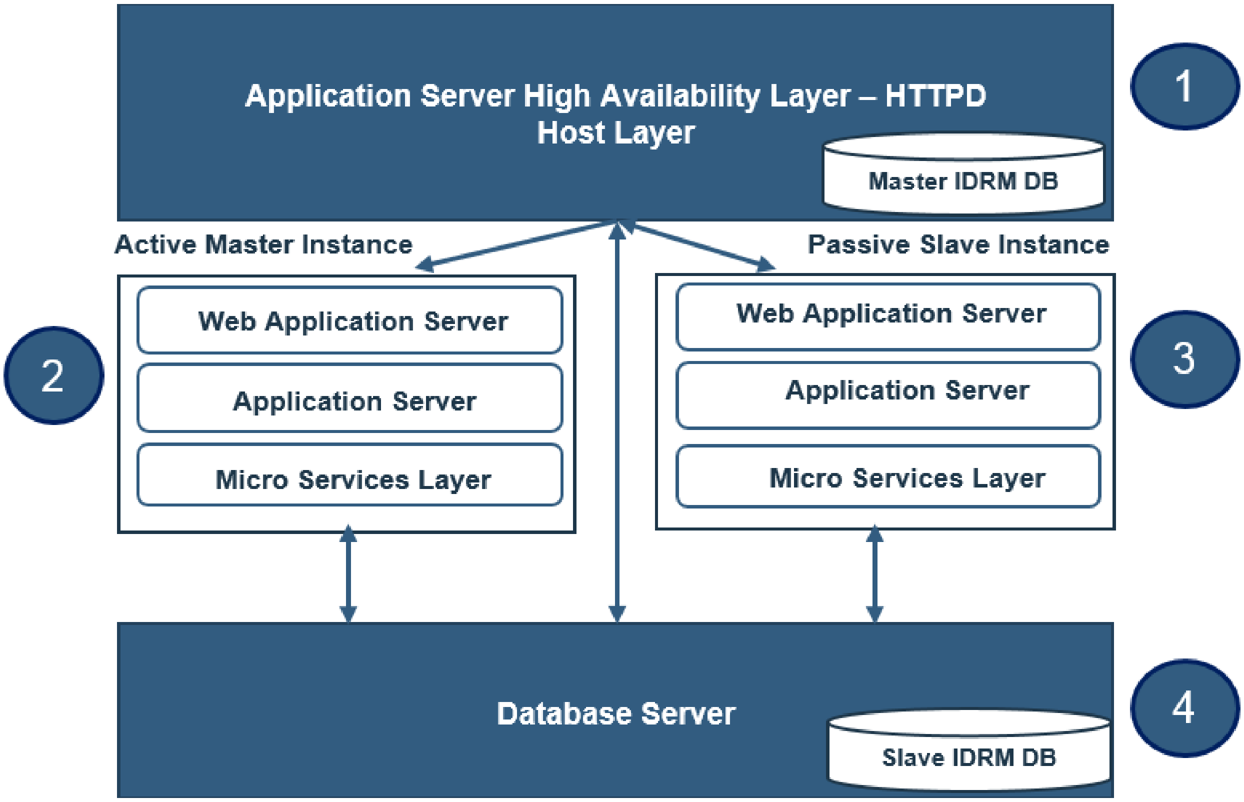
For more information about how to troubleshoot high availability configuration problems, see "High availability configuration problems and workaround" on page 219.

IBM Data Risk Manager high availability deployment model

IBM Data Risk Manager supports four hosts deployment architecture for high availability.

IBM Data Risk Manager high availability deployment model

The following diagram shows IBM Data Risk Manager high availability deployment model. Replication of primary and standby uses WAL(Write-Ahead Log) synchronization and reliability.



Host system requirements high availability deployment

	Host 1	**Host 2**	**Host 3**	**Host 4**
Components	Application Server High Availability Layer and Master Database	IBM Data Risk Manager Application Server (Master)	IBM Data Risk Manager Application Server (Slave)	DB Server (Slave)
Processor	Intel Quad-core XEON 2 GHz or higher	Intel Quad-core XEON 2 GHz or higher	Intel Quad-core XEON 2 GHz or higher	Intel Quad-core XEON 2 GHz or higher
Number of Processors	4	4	4	4
Memory (RAM)	16 GB	16 GB	16 GB	16 GB
Network	Dual 1 Gbps	Dual 1 Gbps	Dual 1 Gbps	Dual 1 Gbps
Storage	200	200	200	200
Operating System	Virtual machine host – VMWare ESXi 5.5 and higher	Virtual machine host – VMWare ESXi 5.5 and higher	Virtual machine host – VMWare ESXi 5.5 and higher	Virtual machine host – VMWare ESXi 5.5 and higher
Architecture	64-bit OS/JVM	64-bit OS/JVM	64-bit OS/JVM	64-bit OS/JVM
Connectivity	Supports internet and intranet	Supports internet and intranet	Supports internet and intranet	Supports internet and intranet

Deployment and Maintenance	Server must be accessible over intranet (through VPN) for installation and configuration.	Server must be accessible over intranet (through VPN) for installation and configuration.	Server must be accessible over intranet (through VPN) for installation and configuration.	Server must be accessible over intranet (through VPN) for installation and configuration.

Configuring Primary Node

You must configure the Primary Node to set up IBM Data Risk Manager high availability. The IBM Data Risk Manager high-availability cluster is made of one Primary Node where the Load Balancing Server and Master Database run.

Before you begin

Ensure that the password for a3user is available.

Before you configure Primary Node, review the considerations and restrictions that are listed in the "Configuring high availability" on page 25 topic.

Procedure

1. Log on to the IBM Data Risk Manager virtual machine (VM) instance that needs to be configured as Primary Node, as a3user, over SSH.
2. Go to the following directory.

   ```
   cd IDRM_HA_Config/
   ```

3. From the command line, run the following script.

   ```
   ./configure_ha
   ```

4. Specify the number of Application Nodes that you want to configure. A maximum of two nodes can be configured.
5. Specify the number of DB Node to be configured. Only one DB Node can be configured.
6. Specify IP address of the Application Nodes.
7. Specify IP address of the DB Node.

   Configuration operation starts only when the specified IP addresses are correct. After the configuration process is complete, an alert message is displayed to configure the DB Node and Application Node before you use IBM Data Risk Manager.

What to do next

Configure the DB Node. For the configuration steps, see "Configuring DB Node" on page 28.

Configuring DB Node

You must configure the DB Node to set up IBM Data Risk Manager high availability. The IBM Data Risk Manager high-availability cluster is made of one DB Node where Slave Database runs.

Before you begin

Ensure that the password for a3user is available.

Before you configure DB Node, review the considerations and restrictions that are listed in the "Configuring high availability" on page 25 topic.

Procedure

1. Log on to the IBM Data Risk Manager virtual machine (VM) instance that needs to be configured as DB Node, as a3user over SSH.

2. Go to the following directory.

   ```
   cd IDRM_HA_Config/
   ```

3. From the command line, run the following script.

   ```
   ./configure_ha
   ```

4. Specify the number of Application Nodes that you want to configure. A maximum of two nodes can be configured. You must specify the same number that you specified during Primary Node configuration.
5. Specify the number of Primary Node to be configured. Only one Primary Node can be configured.
6. Specify IP address of the Application Nodes.
7. Specify IP address of the Primary Node.

   Configuration operation starts only when the specified IP addresses are correct. After the configuration process is complete, an alert message is displayed to indicate that DB Node (Slave Database) is bound to Primary Node (Master Database).

What to do next

Configure the Application Node. For the configuration steps, see "Configuring Application Nodes" on page 29.

Configuring Application Nodes

You must configure the Application Node to set up IBM Data Risk Manager high availability. The IBM Data Risk Manager high-availability cluster can contain a maximum of two Application Nodes.

Before you begin

Ensure that the password for a3user is available.

Before you configure Application Node, review the considerations and restrictions that are listed in the "Configuring high availability" on page 25 topic.

Procedure

1. Log on to the IBM Data Risk Manager virtual machine (VM) instance that needs to be configured as an Application Node, as a3user over SSH.
2. Go to the following directory.

   ```
   cd IDRM_HA_Config/
   ```

3. From the command line, run the following script.

   ```
   ./configure_ha
   ```

4. Specify the number of Primary Node to be configured. Only one Primary Node can be configured.
5. Specify IP address of the Primary Node.

   Configuration operation starts only when the specified IP address is correct. After the configuration process is complete, a message is displayed to indicate that Application Node is bound to Primary Node (load balancer system).

What to do next

After configuration of all the VM instances for high availability, you can access IBM Data Risk Manager by using the following web address.

```
https://PRIMARY_NODE_IP_ADDRESS:8443/albatross/A3Suite
```

You can view the IBM Data Risk Manager high availability status at the following location.

```
https://PRIMARY_NODE_IP_ADDRESS:80/status
```

Administering IBM Data Risk Manager

The administering topics explain configuration and server settings that are needed to perform IBM Data Risk Manager functions seamlessly.

The administrative activities include the following tasks:

- Server settings
- User provisioning
- Adapter configurations
- Other miscellaneous administrative tasks

Before you begin, familiarize yourself with the concepts and terminologies that are mentioned in this section. See the Product overview and Installing and configuring sections for the related information.

IBM Data Risk Manager Administration

Use the IBM Data Risk Manager Administration component to run administrative tasks for setting up and configure various aspects of IBM Data Risk Manager environment. Only the users with `Super Administrator` role can perform administrative operations.

Accessing IBM Data Risk Manager Administration component

1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Click **Administration**.

Following sections describe various options on the **Administration** page to run the administrative tasks.

Diagnostics

Click **Diagnostics** to view status of IBM Data Risk Manager micro services, view micro service log details, configure log levels, and restart the micro service instances.

`Full Stack` is the core IBM Data Risk Manager instance and cannot be modified. To restart a micro service instance, click **Restart**.

Click the **Logs** tab to view and download the log files for a micro service instance. The log files are categorized into four different levels.

Debug
At this level, all the messages from various micro service instances are logged.

Interaction
At this level, all the messages that are generated between server and micro services are logged.

Operational
At this level, all operations across all the micro services are logged.

Warn
At this level, all exceptions across all the micro services are logged. This is the default setting and suggested for production environment.

You can use the **Enable Log Levels** section to dynamically set the log levels.

Manage Load Transactions

Click **Manage Load Transactions** to view the scan details, details of the user who started the scanning process, and date and time at which the scanning process was started.

Audit Logs

Click **Audit Logs** tab to view audit log file details. The file contains details that are related to various users of IBM Data Risk Manager. You can search for specific events from audit logs based on the user name, request type, or activity type.

Server configuration

After the IBM Data Risk Manager installation process is complete, you must perform the initial configurations before it is functional. Click the **Server Configuration** tab to configure the following items.

Email Template Configuration

Configure the template for email notifications.

SMPT Configuration

You can configure IBM Data Risk Manager to send email notifications to the users when events are generated by Database Activity Monitoring (DAM) to take necessary remediation actions. When SMTP is configured, sending email to relevant users on activities or tasks that are associated with a program can be achieved thus seamlessly integrating Action Center functions of IBM Data Risk Manager.

Data Management

Purge Issues – If selected, cleans up alerts or events that are no longer used from the system database. The configuration is set to the duration beyond which the data must be purged. The duration can be specified in number of days, weeks, or months.

Purge Audit Logs – If selected, clean up audit logs from the system database. The audit logs that are generated by IBM Data Risk Manager are accumulates over time and directly impacts the disk space usage. The configuration is set to the duration beyond which the data must be purged. The duration can be specified in number of days, weeks, or months.

Deployment Settings

Defines system-wide operational behavior.

Include CIAR	Select to enable the Confidentiality-Integrity-Availability-Reliability criteria for evaluating information asset risk.
Support Multiple Taxonomy Values	Select to support the multiple taxonomy values.
Transaction Timeout(in minutes)	Represents the maximum time period (in minutes) for IBM Data Risk Manager transaction before timeout occurs.
Schedule Threat Definitions	Configure when or how often the risk scores must be recalculated by the risk engine.
Password Expiry (in Days)	Specify the maximum number of days before a password expires.
Password Policy	Configure to set the policy for password complexity.

SSO and LDAP Configuration

IBM Data Risk Manager can be configured to establish a connection with an LDAP directory or an SSO service provider. You must consider the following points to establish the connection.

- The LDAP directory or SSO service must be running on a host that is accessible to IBM Data Risk Manager server.
- An LDAP account must be available with a user name and password for use by IBM Data Risk Manager.
- You must know the Fully Qualified Domain Name (FQDN) of the LDAP server.

- You must know the port number for IBM Data Risk Manager to communicate with the LDAP server. The default port is 389.
- For SSO, you must provide either the `idp` XML file or the URL of SSO service.
- For a self-signed certificate that is associated with the `idp` file, you must provide the certificate key and password.

For more information about SSO and LDAP configuration, see "LDAP integration with IBM Data Risk Manager" on page 93.

Cross-product integrations

IBM Data Risk Manager can be used with other security products to deliver an integrated solution. Ensure that the configuration settings are correctly done to integrate various external adapters with IBM Data Risk Manager.

Integrating IBM Security Guardium with IBM Data Risk Manager

You can use IBM Data Risk Manager for identifying potential risks to sensitive business information by using IBM Security Guardium Vulnerability Assessment, IBM Security Guardium Database Activity Monitoring, and File Access Monitoring offerings.

IBM Data Risk Manager Integration Exchange (IntEx) agent is used to consume Data Activity Monitoring (DAM) alerts, File Access Monitoring (FAM) alerts, vulnerabilities, and data classification from IBM Security Guardium.

To integrate IBM Security Guardium with IBM Data Risk Manager, run the following tasks.

- Prerequisites
  - Registering IBM Security Guardium.
  - Importing custom report templates into IBM Security Guardium.
  - Sending IBM Security Guardium syslog to the IBM Data Risk Manager Server.
  - Configuring Syslog reporting template.
  - Configuring IBM Data Risk Manager Listener.
- Integrating IBM Security Guardium with IBM Data Risk Manager
- Consuming DAM and FAM alerts in IBM Data Risk Manager
  - Creating DAM and FAM alerts in IBM Security Guardium.
  - Workflow of DAM and FAM alert integration into IBM Data Risk Manager.
  - Importing DAM policies into IBM Data Risk Manager.
  - Mapping IBM Security Guardium DAM and FAM alerts to IBM Data Risk Manager Dashboard.
- Consuming classification data results into IBM Data Risk Manager
  - Importing classifier policies into IBM Data Risk Manager.
  - Importing classifier results CSV file (Catalog data) into IBM Data Risk Manager.
  - Mapping the classification results data to Infrastructure in IBM Data Risk Manager Dashboard.
- Triggering and importing vulnerability assessment into IBM Data Risk Manager
  - Creating IBM Security Guardium data sources in IBM Data Risk Manager.
  - Importing context data.
  - Importing IBM Security Guardium vulnerability assessments (VA) tests.
  - Creating IBM Security Guardium assessment.
  - Viewing IBM Security Guardium assessment scan status.
  - Viewing IBM Security Guardium assessment scan results.

- – Mapping IBM Security Guardium vulnerabilities to Infrastructure on IBM Data Risk Manager Dashboard.
- – Importing IBM Security Guardium vulnerabilities into IBM Data Risk Manager.
- – Importing vulnerabilities as CSV file into IBM Data Risk Manager.

Prerequisite tasks
You must complete the prerequisite tasks to integrate IBM Security Guardium with IBM Data Risk Manager

To integrate IBM Security Guardium with IBM Data Risk Manager, complete the following prerequisites tasks. Ensure that you have the IBM Data Risk Manager Server image or build in the necessary format based on the environment where you are running the installation task. For more information about installation prerequisites, see "Installation prerequisites" on page 17.

- Registering IBM Security Guardium.
- Importing custom report templates into IBM Security Guardium.
- Sending IBM Security Guardium syslog into the IBM Data Risk Manager Server.
- Configuring Syslog reporting template.
- Configuring IBM Data Risk Manager Listener.

Registering IBM Security Guardium

To access data from IBM Security Guardium by using REST APIs, IBM Data Risk Manager server must be registered with IBM Security Guardium appliances. An access code is required for data requisition from and to the IBM Security Guardium appliance. The access code is generated through a secret key (obtained from IBM Security Guardium) by a valid IBM Security Guardium user.

If Central Manager manages all the IBM Security Guardium appliances, Central Manager must be registered with IBM Data Risk Manager Server. When the configuration steps are saved for Central Manager, references to all managed appliances are created automatically.

In Central Manager, use a local CLI-authenticated session to generate a client secret for the application and start the IBM Security Guardium API command to register the client application.

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

In the output, ignore everything except: `client_secret` and `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
```

Save the secret key information for the future and to register with IBM Data Risk Manager Server.

Importing custom report templates into IBM Security Guardium

To view the information about classification processes, vulnerability assessment processes, vulnerability assessment results, and classification results that are run on IBM Security Guardium appliances, custom reports must be created on all the IBM Security Guardium appliances. These custom reports enable IBM Data Risk Manager Server access data on IBM Security Guardium appliances.

Note: Custom reports must be created on all the IBM Security Guardium appliances on which data classification and vulnerability assessment scans are run.

All the ten IBM Security Guardium reports that were received from IBM Data Risk Manager can be imported into the IBM Security Guardium Central Manager.

1. On IBM Security Guardium Central Manager, click **Manage** > **Data Management** > **Definitions Import**.
2. Upload all the ten exported definitions (`.sql` files).

3. Import the uploaded definitions.

Sending IBM Security Guardium syslog into the IBM Data Risk Manager Server

IBM Data Risk Manager server includes a listener component, which monitors activities and events that are collated by configured IBM Security Guardium Collector appliances. IBM Data Risk Manager Server Listener aggregates violations that are reported by the IBM Security Guardium Collector appliances based on the activity monitoring policies, which are installed on the appliances. The IBM Data Risk Manager Server Listener maps the events to the appropriate information and infrastructure assets, which are displayed on IBM Data Risk Manager Dashboard.

Syslog from IBM Security Guardium Collector appliances that monitors the database traffic from database servers must be exported to IBM Data Risk Manager Server. The process of syslog export to IBM Data Risk Manager server must be repeated on all the IBM Security Guardium Collector appliances that are monitoring the database traffic.

Note: The actions that are associated with each database activity monitoring policy must have SYSLOG notification.

From the CLI console of the IBM Security Guardium Collector appliance, run the following command to configure syslog to the IBM Data Risk Manager Server.

```
store remotelog add non_encrypted all.all <ip_address>:<port> tcp
```

Verify the syslog remote store by running the following command.

```
$ show remotelog
Remote syslog is in non-encrypted mode.
*.*    @@<Data Risk Manager_Server_IP>:<port>
ok
```

To clear the syslog remote configuration, run the following command.

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

Restart the Inspection Core and Engines in Central Manager (if Central Manager is present).

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

Configuring Syslog reporting template

In addition, to configure the IBM Security Guardium Collector appliances to send syslog to remote IBM Data Risk Manager Server, message template for the syslog must be modified. For each of the IBM Security Guardium appliance, the message template can be edited in Global Profile of the appliance.

1. Log on to the UI console of the IBM Security Guardium Collector appliance.
2. Go to **Setup** > **Tools and Views**.
3. Select **Global Profile**.
4. In the **Message Template** section of **Global Profile**, copy and paste the following template.

   ```
   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. Click **Apply** to save message template of the syslog.

Configuring IBM Data Risk Manager Listener

For the configuration steps, see "Configuring IBM Security Guardium DAM and FAM Listener" on page 35.

Configuring IBM Security Guardium DAM and FAM Listener

To consume IBM Security Guardium incidents into IBM Data Risk Manager, you must configure Database Activity Monitoring (DAM) and File Access Monitoring (FAM) Listener.

About this task

Listener JAR file can be located at: `/home/a3user/Microservices`

Procedure

1. Open a terminal window.
2. Run the following command.

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

3. When prompted, specify the number of your choice.

   Specify 2 to edit the Listener configuration.
   Specify 1 to connect to IBM Data Risk Manager Server
4. Specify IBM Data Risk Manager Server URL in the following format.

   ```
   https://<server-url>:<port>/albatross
   ```

5. Specify the user name and password with appropriate privileges to connect to IBM Data Risk Manager Server.
6. Select the organization when prompted.

   Note: Selecting the organization is mandatory. Listener maps all the Database Activity Monitoring logs to the selected organizations.
7. Specify option 2 to configure IBM Security Guardium syslog port settings.

   Specify the syslog port where IBM Security Guardium appliances are sending syslog files to the IBM Data Risk Manager Server – 9003.
8. Start IBM Data Risk Manager DAM/FAM Listener by running the following command.

   ```
   sudo service listener start
   ```

Integrating IBM Security Guardium with IBM Data Risk Manager

Configure IBM Data Risk Manager to communicate with IBM Security Guardium to use its sensitive data-related risk information in IBM Data Risk Manager for analysis.

Before you begin

Ensure that the secret key and the client identifier are available, which is needed to establish the connection with IBM Security Guardium. Use the IBM Security Guardium command line interface to generate a secret key to IBM Data Risk Manager Server.

1. Log on to the command line interface of IBM Security Guardium.

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

2. Generate a secret key for the application, and start Guardium API command to register the client application.

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

About this task

The Business Context Modeler (BCM) component of IBM Data Risk Manager provides Enterprise Integration Wizard to integrate IBM Security Guardium with IBM Data Risk Manager.

Procedure

1. Log in to IBM Data Risk Manager Application Suite by using your user credentials.
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
4. In the Adapter Configuration section, click the **Add Integration Adapter** icon ⊕.
5. Select **IBM Guardium** from the list.
6. To add an IBM Security Guardium instance, select **IBM Guardium** from the Adapter Configuration list.
7. In the Integration Instances section, click the **Add Instance** icon ⊕.
8. Set the following options.

Option	Description
Name	Specify a name for IBM Security Guardium instance.
URL	Specify the URL to access IBM Security Guardium, for example `https://<Guardium appliance-IP/host name:Port>`.
Microservice Instance	Select the agent that is needed for integration. For example, `guardium-integration-intex`.
Guardium Type	Select any of the following IBM Security Guardium systems for accessing and importing data objects. • **Central Manager** • **Aggregator** • **Collector**
User Name	Specify the IBM Security Guardium user name with administrator role.
Password	Specify the password for the user name.

Option	Description
Guardium Client ID	Specify the client ID to connect to IBM Security Guardium.
Guardium Client Secret Key	Specify the secret key to establish connection with IBM Security Guardium.
Run VA	Select to run the vulnerability assessment scan.
Classifier and Vulnerability Assessment	Specify the configuration file to import data from integration server to IBM Data Risk Manager for data classification and vulnerability assessments.
Feeds	Specify the configuration file to retrieve syslog feeds (alert events) from integration server. These alert events are mapped to the appropriate information assets and infrastructure in IBM Data Risk Manager to view them on the dashboard.

9. Click **Save** to save the configuration details.

What to do next

For the adapter instance that you created, you can test the connectivity. Select the instance from the **Integration Instances** list, and then click **Test Connection** to test whether the communication between IBM Security Guardium instance and IBM Data Risk Manager server is successful.

You can import managed units of the adapter instance that you created. Select the adapter instance, and then click **Get Managed Units**.

Consuming DAM and FAM alerts into IBM Data Risk Manager

You must run various tasks to use the Database Activity Monitoring (DAM) and File Access Monitoring (FAM) alerts in IBM Data Risk Manager.

To create and use DAM and FAM alerts in IBM Data Risk Manager, run the following tasks.

- Creating DAM and FAM alerts in IBM Security Guardium.
- Importing DAM policies into IBM Data Risk Manager.
- Mapping IBM Security Guardium DAM and FAM alerts to IBM Data Risk Manager Dashboard.

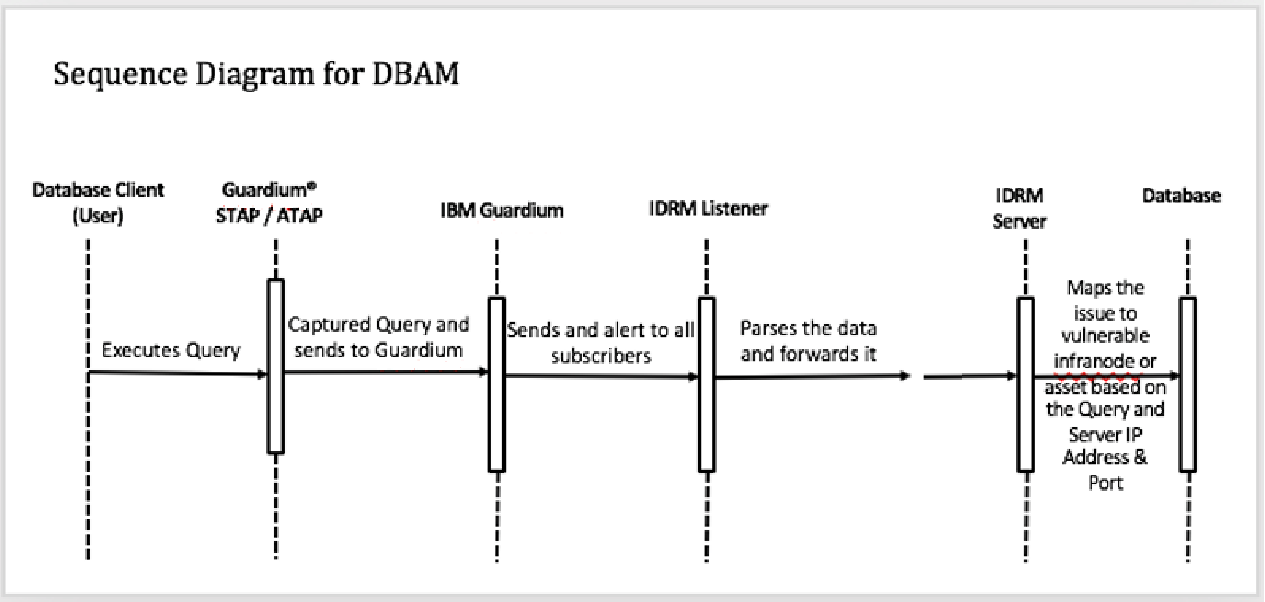
Creating DAM and FAM alerts in IBM Security Guardium

Install STAP on the database servers where the risks are monitored and assessed.

DAM Policy access rules are created in IBM Security Guardium and deployed on STAP. Based on a rule combination, if you trigger an SQL query, STAP sends the captured query to IBM Security Guardium. IBM Security Guardium then sends the DAM alerts through syslog interface to IBM Data Risk ManagerListener, which then parses the data and forwards to the server.

Workflow of DAM and FAM alert integration into IBM Data Risk Manager

The following diagram shows the workflow of DAM and FAM alert integration into IBM Data Risk Manager.


Sequence Diagram for DBAM
Database Client (User)
Guardium® STAP / ATAP
IBM Guardium
IDRM Listener
IDRM Server
Database
Executes Query
Captured Query and sends to Guardium
Sends and alert to all subscribers
Parses the data and forwards it
Maps the issue to vulnerable infranode or asset based on the Query and Server IP Address & Port

Server maps the issue to vulnerable infra node or asset based on the Query, Server IP address, and port.

For FAM, FTAP gets installed on the file server. Any fraudulent access to file happens on the server based on the FAM policy rule that is deployed on the collector appliance. Appropriate FAM alerts get routed from file server to IBM Security Guardium.

Importing DAM policies into IBM Data Risk Manager

For the steps on how to import DAM policies, see "Importing Database Activity Monitoring policies into IBM Data Risk Manager" on page 38.

Mapping IBM Security Guardium DAM and FAM alerts to IBM Data Risk Manager Dashboard

1. Trigger IBM Security Guardium or unstructured scan on any of the inventories on which STAP or FTAP is installed.
2. Import context data and apply the taxonomy attributes.
3. Export the information asset to dashboard.
4. When the SQL query runs and satisfies DAM rule, DAM alerts from IBM Security Guardium are routed to IBM Data Risk Manager server.
5. When the file activity gets executed and satisfies FAM rule, FAM alerts from IBM Security Guardium are routed to the IBM Data Risk Manager server.
6. Corresponding DAM and FAM alerts are mapped to the appropriate infrastructures in IBM Data Risk Manager, which can be viewed on the **Incidents** tab in the Information Asset secondary details page. The number of DAM and FAM alerts can also be viewed in the **Infrastructure** tab correlating to number of alerts with the inventory as Database, which has STAP monitor icon.

Importing Database Activity Monitoring policies into IBM Data Risk Manager

You can import Database Activity Monitoring (DAM) policies from IBM Security Guardium appliances into IBM Data Risk Manager inventory for data classification and risk analysis.

About this task

The transaction icon ⇅✓ indicates that the previous import operation was successful.

The transaction icon ⇅! indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Policies**.
4. Import policies.

   a) Click the **Download** icon .

   b) On the **Import** window, select **Security**.

   c) From the **Instances** list, select an adapter instance.

   d) Click **Import**. When the import operation is complete, the IBM Security Guardium policies are added to the inventory.

   e) To refresh policy inventory list, click the **Refresh** icon .

Consuming classification data results in IBM Data Risk Manager

You must run various tasks to use classification data results in IBM Data Risk Manager.

To use the classification data results in IBM Data Risk Manager, run the following tasks.

- Importing classifier policies into IBM Data Risk Manager.
- Importing classifier results CSV file (Catalog data) into IBM Data Risk Manager.
- Mapping the classification results data to Infrastructure in IBM Data Risk Manager Dashboard.

Importing classifier policies into IBM Data Risk Manager

You can import classifier policies if the policies are created in IBM Security Guardium. For the steps on how to import policies, see "Importing classifier policies into IBM Data Risk Manager" on page 39.

Importing classifier results CSV file (Catalog data) into IBM Data Risk Manager.

For the steps on how to import classifier results CSV file (Catalog data) into IBM Data Risk Manager, see "Importing classifier results CSV file (catalog data) into IBM Data Risk Manager" on page 40

Mapping the classification results data to Infrastructure in IBM Data Risk Manager Dashboard.

1. Trigger IBM Security Guardium meta scan on any of the systems where IBM Security Guardium inventory is created.
2. Import context data and apply the taxonomy attributes.
3. Export the information asset to IBM Data Risk Manager Dashboard.
4. Corresponding classifier results are mapped to the appropriate Infrastructure in IBM Data Risk Manager. The results can be viewed on Information Asset Details, in the Infrastructure widget that shows the data asset percentage.

Importing classifier policies into IBM Data Risk Manager

You can import classifier policies from IBM Security Guardium appliances into IBM Data Risk Manager inventory for data classification and risk analysis.

About this task

The transaction icon ✓ indicates that the previous import operation was successful.

The transaction icon ! indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Policies**.
4. Import classifier policies.

   a) Click the **Download** icon .

   b) On the **Import** window, select **Classifier**.

   c) From the **Instances** list, select an adapter instance.

   d) Click **Import**. When the import operation is complete, the IBM Security Guardium policies are added to the inventory.

   e) To refresh policy inventory list, click the **Refresh** icon .

Importing classifier results CSV file (catalog data) into IBM Data Risk Manager

Use the Business Context Modeler component of IBM Data Risk Manager to import classifier results as CSV file into IBM Data Risk Manager.

Before you begin

Ensure that the business context data is available for importing.

You can download the sample templates at: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**.
4. Enable the **Catalog Data** toggle button.
5. Select **Classification**.
6. Click **Choose File** to locate and select the file.
7. Click **Load**.

   Data is displayed for your verification.
8. Click **Import**.

Triggering and importing vulnerability assessment into IBM Data Risk Manager

You must run various tasks to trigger and import vulnerability assessment into IBM Data Risk Manager.

To trigger and import vulnerability assessment into IBM Data Risk Manager, run the following tasks.

- Creating IBM Security Guardium data sources in IBM Data Risk Manager.
- Importing context data.
- Importing IBM Security Guardium vulnerability tests.
- Creating IBM Security Guardium assessment.
- Viewing IBM Security Guardium assessment scan status.
- Viewing IBM Security Guardium assessment scan results.
- Mapping IBM Security Guardium vulnerabilities to Infrastructure on IBM Data Risk Manager Dashboard.

- Importing IBM Security Guardium vulnerabilities into IBM Data Risk Manager.
- Importing vulnerabilities as CSV file into IBM Data Risk Manager.

Creating IBM Security Guardium data sources in IBM Data Risk Manager

For the steps on how to create the data sources, see "Adding IBM Security Guardium data sources" on page 42.

Importing context data

Import context data. Ensure that the context data is saved properly and the attributes are mapped to the appropriate inventory that was created earlier. For more information about importing context data, see "Mapping business context data" on page 99.

Note: Inventory can be created in IBM Data Risk Manager by providing the data source name and type in the context data `Database` sheet.

Importing IBM Security Guardium vulnerability assessments (VA) tests

For the steps on how to import VA tests, see "Importing IBM Security Guardium vulnerability assessment tests" on page 42

Creating IBM Security Guardium assessment

For the steps on creating an assessment, see "Creating and triggering vulnerability assessment scan" on page 43

Viewing IBM Security Guardium assessment scan status

For the steps on how to view status, see "Viewing scan status" on page 53.

Viewing IBM Security Guardium assessment scan results

For the steps on how to view scan results, see "Viewing vulnerability assessment scan results for IBM Security Guardium" on page 44.

Mapping IBM Security Guardium vulnerabilities to Infrastructure on IBM Data Risk Manager Dashboard

When the scan results are completed on the Vulnerability dashboard, you can view the vulnerability scan results on the IBM Data Risk Manager dashboard. Click the Information Asset secondary page to view the IBM Security Guardium vulnerabilities of the endpoint inventory. Infrastructure vulnerability count is shown on the Infrastructure widget.

Importing IBM Security Guardium vulnerabilities into IBM Data Risk Manager

For the steps on how to import vulnerabilities, see Importing vulnerability scans.

Importing vulnerabilities as CSV file into IBM Data Risk Manager

You can import vulnerabilities as CSV file into IBM Data Risk Manager. For the steps on how to import the CSV file, see Importing vulnerability scans.

Remediating vulnerabilities

When the vulnerabilities are identified through scans, remediation actions must be taken to evaluate the correct risk exposure for the information asset. For the steps on how to define remediation actions, see "Creating an activity to remediate vulnerabilities" on page 45.

Adding IBM Security Guardium data sources

You can add IBM Security Guardium data sources into IBM Data Risk Manager inventory to make the data available for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security Guardium. For more information about integration, see "Integrating IBM Security Guardium with IBM Data Risk Manager" on page 36.

Before you create a data source, you must be aware of the database connection parameters for the data source you want to connect to.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.
4. To add IBM Security Guardium data source, click the **Add Data Source** icon ⊕.
5. On the **Add Data Source** page, set the following options and click **Add**.

Option	**Description**
Server Type	Database server type that you want to use. For example, `MySQL`.
Data Source Name	A unique name for the data source.
IP Address	IP address of the database server.
Port	Listening port number of the data source.
Database Name	Name of the database.
Adapter	IBM Security Guardium instance name. For example, `Guardium_Adapter`.
Agents	Agent name to connect to the database.
User Name	Name of the user for connecting to the database.
Password	Password for the database user name.
Encryption	Encryption status of the data source server.
Monitoring	Status of database monitoring agent, such as S-TAP.
Custom URL	Custom URL connection string to the data source.
Geographic Location	Geographic location of the data source.

The data source that you added is listed on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **Database**.

Importing IBM Security Guardium vulnerability assessment tests

Import IBM Security Guardium vulnerability assessment (VA) tests into IBM Data Risk Manager for data analysis.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.

2. Click the application navigation icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **VA Tests**.
4. To download scan templates, click the **Download** icon .
5. On the **Import** window, select an adapter instance for IBM Security Guardium.
6. Click **Import**. When the import operation is complete, VA tests are added to the inventory.
7. To refresh VA test inventory list, click the **Refresh** icon .

Creating and triggering vulnerability assessment scan

Use the Vulnerability Management component of IBM Data Risk Manager to create and run the assessment scan in IBM Security Guardium to identify vulnerabilities in databases.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security Guardium. For more information about integration, see "Integrating IBM Security Guardium with IBM Data Risk Manager" on page 36.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Click **Vulnerability Management**.
4. Select a program from the list.
5. Click **Create New Assessment**.
6. On the **Create New Assessment** page, set the following options and click **Create Assessment**.

Option	Description
Assessment Name	IBM Security Guardium vulnerability assessment name.
Scan Type	Scan type, for example, `Database Scanner`.
Platform	Database type selection for running the vulnerability assessment process.
Run on	IBM Security Guardium adapter instance for running the vulnerability assessment process. List contains only the instances for which option **Run VA** is selected when the integration instance is created.

7. Under **Scope of Assessment**, add data sources to the transaction based on the scope or last scan days. You can add multiple data sources.
8. Click **Add Scope to Transaction**.
9. Select vulnerability tests from the list and click **Save**.
10. Under **Pending Transactions** on the Transaction View, click the **Start Process** icon .
11. Select **Scan Now**.

    To schedule the scan later, select **Scan Later**.

    To save transaction details after completion of the process under **Pending Transactions** for reuse, select **Replica**.
12. To start the process, click the **Trigger Assessment** icon .

Viewing vulnerability assessment scan results for IBM Security Guardium

Use the Vulnerability Assessment component of IBM Data Risk Manager to view vulnerability assessment scan results for further analysis and actions.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Click **Vulnerability Management**.
4. Click **Results View**.
5. Click the filter icon under **VA Data Sources**, and select the adapter type, for example, `IBM Guardium`.
6. For the selected assessment, click the number for **Pass**, **Fail** or **Others** to display results in the **Vulnerabilities Test Results** page.
7. To view results based on the platform, click **VA Platforms**.

Importing IBM Security Guardium vulnerabilities into IBM Data Risk Manager

You can import vulnerability scans from IBM Security Guardium into IBM Data Risk Manager inventory for risk analysis.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security Guardium. For more information about integration, see "Integrating IBM Security Guardium with IBM Data Risk Manager" on page 36.

About this task

The transaction icon indicates that the previous import operation was successful.

The transaction icon indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Scans**.
4. Import data scans.

   a) Click the **Download** icon .

   b) On the **Import** window, select **Vulnerability Assessment**.

   c) From the **Adapter** list, select **IBM Guardium**.

   d) From the **Instances** list, select an adapter instance. You can select up to three instances.

   e) Select the date from which you need to pull vulnerability assessment scans from IBM Security Guardium.

   f) Click **Import**. When the import operation is complete, the IBM Security Guardium vulnerability assessment scans are added to the inventory.
5. On the **Data Scans** page, you can view the scans that you now imported.
6. To refresh data scan inventory list, click the **Refresh** icon .

7. Alternatively, to view scan results after the import operation, go to **Security Command and Control Center** > **Home**.

Importing vulnerabilities as CSV file into IBM Data Risk Manager

Use the Business Context Modeler component of IBM Data Risk Manager to import vulnerabilities as CSV file into IBM Data Risk Manager.

Before you begin

Ensure that the business context data is available for importing.

You can download the sample templates at: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**.
4. Enable the **Catalog Data** toggle button.
5. Select **Vulnerability**.
6. Click **Choose File** to locate and select the file.
7. Click **Load**.

   Data is displayed for your verification.
8. Click **Import**.

Creating an activity to remediate vulnerabilities

Use the Vulnerability Management component of IBM Data Risk Manager to view and remediate vulnerabilities. When the vulnerabilities are identified through scans, remediation actions must be taken to evaluate the correct risk exposure for the information asset.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Click **Vulnerability Management**.
4. Go to **Results View**.
5. Click **VA Data Sources**.
6. Click the filter icon under **VA Data Sources**, and select your adapter type, for example, `IBM QRadar`.
7. Alternatively, you can select a data source based on the platform.
   a) Click **VA Platforms**.
   b) Select a platform and click the database icon to select your data source.
8. For a selected data source, click the number for **Fail** to display results in the **Vulnerabilities Test Results** page.
9. Click the down arrow icon to select the severity level.
10. Click the **Remediation** icon .

11. Click **Yes** to create remediation actions.
12. On the **Create Remediation Activity** window, specify the necessary information. If the data source is from ServiceNow, you can publish the activity as an incident on ServiceNow for remediation management.
13. Click **Create**.

    On the **Vulnerabilities Test Results** page, under **Activity**, you can view activity details if the end date of activity is greater than the execution date of test results.

What to do next

You can view and manage the remediation activities that you defined in the following areas.

IBM Data Risk Manager Action Center

- Click the application menu icon.
- Click **Action Center**.

For more information about Action Center, see "Action Center" on page 140.

Asset Details window on IBM Data Risk Manager Dashboard

- Click the application menu icon.
- Click **Dashboard**.
- On the **Information Asset Portfolio** window, click the arrow icon on the asset to view the asset details.
- On the **Asset Details** window, click **Infrastructure** > **Vulnerabilities**.
- To view action items, select the infrastructure node and click **Action Items**.

Exporting cleansed IBM Security Guardium data sources to dashboard

You can directly export the cleansed IBM Security Guardium data source to IBM Data Risk Manager Dashboard. You must import the classifier scan from IBM Security Guardium where scan is run on the data source that you want to export.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security Guardium. For more information about the integration steps, see "Integrating IBM Security Guardium with IBM Data Risk Manager" on page 36.

Ensure that the necessary IBM Security Guardium classifier scans are imported to IBM Data Risk Manager inventory. For more information about how to import the scan, see "Importing classifier scans from IBM Security Guardium" on page 133.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Scans**.
4. Select the classifier scan, which is run on the data source that you want to export to IBM Data Risk Manager Dashboard.
5. Click the export icon.
6. Click **Yes** to confirm the export operation.

   The export icon on the selected data scan indicates that the scan is exported to dashboard.

Click the information icon ••• to view the number of data sources, tables, and columns that are associated with the selected scan.

7. Select your program from the list.
8. View the data source that you exported to IBM Data Risk Manager Dashboard.
   a) Go to **Business Context Modeler** > **Dashboard**.
   b) Click **Program** to select your program.
   c) Click **Dashboard** to view the asset.

File Activity Monitoring
File Activity Monitoring (FAM) discovers sensitive data on your servers. The data discovery includes collection of metadata and entitlements for files and folders.

FAM includes the following activities:

- Classifies the content by using pre-defined or user-defined definitions.
- Configures rules and policies about data access, and actions to be taken when rules are met.
- Scales with growing data volumes and expanding enterprise requirements.
- Provides extensive heterogeneous support across all popular data systems.

FAM consists of the following capabilities:

- Tracks the user activities, such as modification or deletion of content on files and folders.
- Tracks all the database-related activities on files and folders.
- Notifies administrators and owners about the database operations that are performed on files and folders.

Integrating IBM QRadar Security Intelligence Platform with IBM Data Risk Manager

The events that are marked as offense in IBM QRadar Security Intelligence Platform are imported into IBM Data Risk Manager. These events are consumed as threat in IBM Data Risk Manager, then mapped into appropriate infrastructure for analysis and assessments.

IBM Data Risk Manager Integration Exchange (IntEx) agent is used to consume application vulnerabilities from IBM Security AppScan EnterpriseIBM QRadar Security Intelligence Platform.

For more information about installation prerequisites, see "Installation prerequisites" on page 17.

To consume IBM QRadar Security Intelligence Platform offenses into IBM Data Risk Manager, and to import IBM QRadar Security Intelligence Platform vulnerability assessment into IBM Data Risk Manager, run the following tasks.

- Consuming IBM QRadar Security Intelligence Platform offenses into IBM Data Risk Manager.
  - Creating offenses in IBM QRadar Security Intelligence Platform.
  - Workflow of offenses integration into IBM Data Risk Manager.
  - Integrating IBM QRadar Security Intelligence Platform with IBM Data Risk Manager.
  - Configuring IBM QRadar Security Intelligence Platform SIEM Listener.
  - Mapping IBM QRadar Security Intelligence Platform offenses to Infrastructure in IBM Data Risk Manager Dashboard.
- Triggering and importing IBM QRadar Security Intelligence Platform vulnerability assessment into IBM Data Risk Manager.
  - Creating endpoint inventory in IBM Data Risk Manager.
  - Importing context data.
  - Creating endpoint assessment.
  - Viewing endpoint assessment scan status.
  - Viewing endpoint assessment scan results.

- Mapping endpoint vulnerabilities to Infrastructure on IBM Data Risk Manager Dashboard.
- Importing endpoint vulnerabilities into IBM Data Risk Manager.

Creating offenses in IBM QRadar Security Intelligence Platform

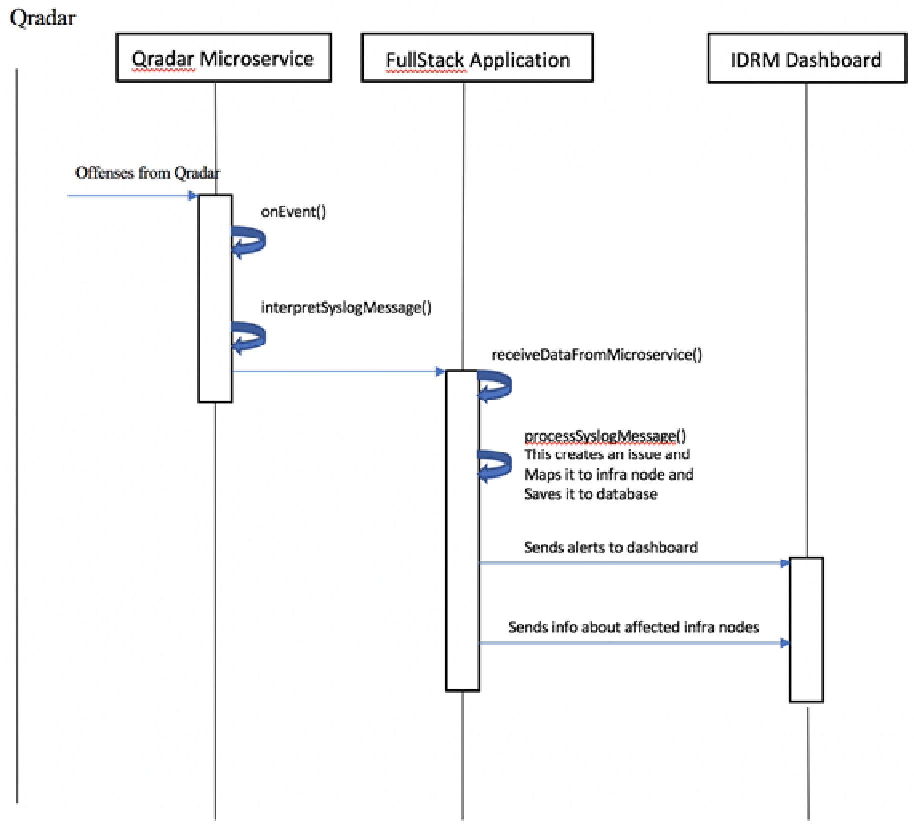
To collect events from IBM QRadar Security Intelligence Platform, install the Win collect agent on Windows system. Enable syslog for non-Windows system

After the Win collect agent is installed on Windows systems and IBM QRadar Security Intelligence Platform is configured by creating a log source, the events are available as a log activity.

Workflow of offenses integration into IBM Data Risk Manager

IBM QRadar Security Intelligence Platform creates the offense based on the custom rule that was created in the appliance on a specific risk factor, for example time. An offense can be created if the events are happening on those specific time window.

When these offenses are consumed into IBM Data Risk Manager, IBM Data Risk Manager SIEM micro service, interprets those syslog messages and sends them to the server. The data is then processed, issue is created, and mapped to the appropriate Infrastructure. The following diagram shows the workflow of offenses.



Integrating IBM QRadar Security Intelligence Platform with IBM Data Risk Manager.

Configure IBM Data Risk Manager to communicate with IBM QRadar Security Intelligence Platform. For the configurations steps, see Integrating IBM QRadar Security Intelligence Platform with IBM Data Risk Manager.

Configuring IBM QRadar Security Intelligence Platform SIEM Listener

To consume IBM QRadar Security Intelligence Platform offenses into IBM Data Risk Manager, you must configure SIEM Listener. For the configuration steps, see “Configuring IBM QRadar Security Intelligence Platform SIEM Listener” on page 51.

Mapping IBM QRadar Security Intelligence Platform offenses to Infrastructure in IBM Data Risk Manager Dashboard

To map IBM QRadar Security Intelligence Platform offenses to Infrastructure in IBM Data Risk Manager Dashboard, run the following steps.

1. Trigger the scan on any of the inventory on which the Win collect agent is installed.
2. Import context data, apply the taxonomy attributes, and export the information asset to IBM Data Risk Manager Dashboard.

   When the listener is up and appropriate custom rules are set up in IBM QRadar Security Intelligence Platform, the offenses are generated and sent to IBM Data Risk Manager.
3. The offenses that are mapped to Infrastructure in IBM Data Risk Manager Dashboard, can be viewed on the **Offenses** tab in the **Information Asset** secondary details page. You can also view the number of offenses in the **Infrastructure** tab that are associated with number of alerts with the inventory being the endpoint.

Creating endpoint inventory in IBM Data Risk Manager

Add IBM QRadar Security Intelligence Platform endpoint inventory into IBM Data Risk Manager. For the steps on how to add the inventory, see "Adding IBM QRadar Security Intelligence Platform data sources" on page 51.

Importing context data

Import context data. Ensure that the context data is saved properly and the attributes are mapped to the appropriate inventory that was created earlier. For more information about importing context data, see "Mapping business context data" on page 99.

Note: Inventory can be created in IBM Data Risk Manager by providing the data source name and type in the context data `Database` sheet.

Creating endpoint assessment

Use the Vulnerability Assessment component of IBM Data Risk Manager to create endpoint assessment. For the steps on how to create endpoint assessment, see "Creating and triggering an endpoint assessment scan" on page 52.

Viewing endpoint assessment scan status

You can view the application assessment scan status to proceed with further analysis and actions. For the steps on how to view the scan status, see Viewing scan status.

Viewing endpoint assessment scan results

View endpoint assessment scan results for further analysis and actions. For the steps on how to view the scan results, see Viewing scan results.

Mapping endpoint vulnerabilities to Infrastructure on IBM Data Risk Manager Dashboard

When the application assessment scan is successfully completed, you can view the vulnerability scan results on IBM Data Risk Manager Dashboard. Go to the Information Asset secondary page to view the endpoint vulnerabilities of the endpoint inventory. Infrastructure vulnerability count is shown on the Infrastructure widget. For more information about the dashboard, see "IBM Data Risk Manager Dashboard" on page 164.

Importing endpoint vulnerabilities into IBM Data Risk Manager

Import vulnerability scans from IBM QRadar Security Intelligence Platform appliances into IBM Data Risk Manager inventory for data classification and risk analysis. For the steps on how to import the scan, see Importing vulnerability scans.

Note: While importing the scans, data sources and scan results are also imported.

Importing endpoint vulnerabilities into IBM Data Risk Manager

You can import endpoint vulnerabilities as CSV file into IBM Data Risk Manager. For the steps on how to import the CSV file, see Importing vulnerabilities as CSV file into IBM Data Risk Manager.

Remediating vulnerabilities

When the vulnerabilities are identified through scans, remediation actions must be taken to evaluate the correct risk exposure for the information asset. For the steps on how to define remediation actions, see “Creating an activity to remediate vulnerabilities” on page 45.

Integrating IBM QRadar Security Intelligence Platform with IBM Data Risk Manager

Configure IBM Data Risk Manager to communicate with IBM QRadar Security Intelligence Platform to use its sensitive data-related risk information in IBM Data Risk Manager for analysis.

About this task

The Business Context Modeler (BCM) component of IBM Data Risk Manager provides Enterprise Integration Wizard to integrate IBM QRadar Security Intelligence Platform with IBM Data Risk Manager.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
4. In the Adapter Configuration section, click the **Add Integration Adapter** icon ⊕.
5. Select **IBM QRadar** from the list.
6. To add an IBM QRadar Security Intelligence Platform instance, select **IBM QRadar** from the Adapter Configuration list.
7. In the Integration Instances section, click the **Add Instance** icon ⊕.
8. Set the following options.

Option	Description
Name	Specify a name for IBM QRadar Security Intelligence Platform instance.
URL	Specify the URL to access IBM QRadar Security Intelligence Platform, for example `https://<qradar application-IP/host name:Port>`.
Microservice Instance	Select the agent that is needed for integration.
User Name	Specify the IBM QRadar Security Intelligence Platform user name with administrator role.
Password	Specify the password for the user name.
Classifier and Vulnerability Assessment	Specify the configuration file to import data from integration server to IBM Data Risk Manager for data classification and vulnerability assessments.
Feeds	Specify the configuration file to retrieve syslog feeds (alert events) from integration server. These alert events are mapped to the appropriate information assets and infrastructure in IBM Data Risk Manager to view them on the dashboard.

9. Click **Save** to save the configuration details.

What to do next

For the adapter instance that you created, you can test the connectivity. Select the instance from the **Integration Instances** list, and then click **Test Connection** to test whether the communication between IBM QRadar Security Intelligence Platform instance and IBM Data Risk Manager server is successful.

Configuring IBM QRadar Security Intelligence Platform SIEM Listener

To consume IBM QRadar Security Intelligence Platform offenses into IBM Data Risk Manager, you must configure SIEM Listener.

About this task

Listener JAR file can be located at: `/home/a3user/Micro services`

Procedure

1. Open a terminal window.
2. Run the following command.

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

3. When prompted, specify the number of your choice.

   Specify 2 to edit the Listener configuration.
   Specify 1 to connect to IBM Data Risk Manager Server
4. Specify IBM Data Risk Manager Server URL in the following format.

   ```
   https://<server-url>:<port>/albatross
   ```

5. Specify the user name and password with appropriate privileges to connect to IBM Data Risk Manager Server.
6. Select the organization when prompted.

   Note: Selecting the organization is mandatory. Listener maps all the Database Activity Monitoring logs to the selected organizations.
7. Specify option 2 to configure IBM QRadar Security Intelligence Platform syslog port settings.

   Specify the syslog port where IBM QRadar Security Intelligence Platform appliances are sending syslog files to the IBM Data Risk Manager Server – 9000.
8. Start IBM Data Risk Manager QRadar Listener by running the following command.

   ```
   sudo service qradar start
   ```

Adding IBM QRadar Security Intelligence Platform data sources

You can add IBM QRadar Security Intelligence Platform data sources into IBM Data Risk Manager inventory for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM QRadar Security Intelligence Platform. For more information about integration, see Integrating IBM QRadar Security Intelligence Platform with IBM Data Risk Manager.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.

4. To add IBM QRadar Security Intelligence Platform data source, click the **Add Data Source** icon ⊕.
5. On the **Add Data Source** page, set the following options and click **Add**.

Option	Description
Server Type	Data source server type that you want to use, for example `Server`.
Data Source Name	Name for the data source.
IP Address	IP address of the data source server.
Adapter	IBM QRadar Security Intelligence Platform instance name. For example, `Qradar_Adapter`.
Agents	Agent name to connect to the data source.
User Name	Name of the user.
Password	Password for the user name.
Encryption	Encryption status of the data source server.
Monitoring	Status of the monitoring agent.
Geographic Location	Geographic location of the data source.

The data source that you added is listed on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **Server**.

Creating and triggering an endpoint assessment scan

Use the Vulnerability Management component of IBM Data Risk Manager to create and run the assessment scan in IBM QRadar Security Intelligence Platform to identify endpoint vulnerabilities.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM QRadar Security Intelligence Platform. For more information about integration, see "Integrating IBM QRadar Security Intelligence Platform with IBM Data Risk Manager" on page 50.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Click **Vulnerability Management**.
4. Select a program from the list.
5. Click **Create New Assessment**.
6. On the **Create New Assessment** page, set the following options and click **Create Assessment**.

Option	Description
Assessment Name	IBM QRadar Security Intelligence Platform endpoint assessment name.
Scan Type	Scan type, for example, `Server Vulnerability Scanner`.
Run on	IBM QRadar Security Intelligence Platform adapter instance for running the vulnerability assessment process.

7. Under **Scope of Assessment**, add data sources to the transaction based on the scope or last scan days. You can add multiple data sources.
8. Click **Add Scope to Transaction**.

9. Under **Pending Transactions** on the Transaction View, click the **Start Process** icon .
10. Select **Scan Now**.

    To schedule the scan later, select **Scan Later**.

    To save transaction details after completion of the process under **Pending Transactions** for reuse, select **Replica**.
11. To run the process, click the **Trigger Assessment** icon .

Viewing scan status

Use the Security Command and Control Center (SC3) component of IBM Data Risk Manager to view the vulnerability assessment scan status for further analysis and actions.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the menu icon .
3. Select a program from the list.
4. Go to **Security Command and Control Center** > **Home**.
5. To view the list of completed processes along with the status, click **Vulnerability Assessment Processes**.

Viewing IBM QRadar Security Intelligence Platform endpoint assessment scan results

Use the Vulnerability Assessment component of IBM Data Risk Manager to view endpoint assessment scan results for further analysis and actions.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Click **Vulnerability Management**.
4. Click **Results View**.
5. Click the filter icon under **VA Data Sources**, and select the adapter type, for example, `IBM QRadar`.
6. For the selected assessment, click the number for **Pass**, **Fail** or **Others** to display results in the **Vulnerabilities Test Results** page.

Importing vulnerability scans from IBM QRadar Security Intelligence Platform

You can import vulnerability scans from IBM QRadar Security Intelligence Platform appliances into IBM Data Risk Manager inventory for risk analysis.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM QRadar Security Intelligence Platform. For more information about integration, see "Integrating IBM QRadar Security Intelligence Platform with IBM Data Risk Manager" on page 50.

When you trigger the VA scan from IBM Data Risk Manager, if the scan fails in IBM Data Risk Manager and completes in IBM QRadar Security Intelligence Platform, you cannot import those scans as there is no data source concept in IBM QRadar Security Intelligence Platform. IBM QRadar Security Intelligence Platform has the concept of Asset, which has the endpoint IP address.

About this task

The transaction icon indicates that the previous import operation was successful.

The transaction icon indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Scans**.
4. Import data scans.
   a) Click the **Download** icon .
   b) On the **Import** window, select **Vulnerability Assessment**.
   c) From the **Adapter** list, select **IBM QRadar**.
   d) From the **Instances** list, select an adapter instance. You can select up to three instances.
   e) Click **Import**. When the import operation is complete, the IBM QRadar Security Intelligence Platform scans are added to the inventory.
   f) To refresh data scan inventory list, click the **Refresh** icon .
5. To view results after the import operation, go to **Security Command and Control Center** > **Home**.

Importing vulnerabilities as CSV file into IBM Data Risk Manager

Use the Business Context Modeler component of IBM Data Risk Manager to import vulnerabilities as CSV file into IBM Data Risk Manager.

Before you begin

Ensure that the business context data is available for importing.

You can download the sample templates at: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**.
4. Enable the **Catalog Data** toggle button.
5. Select **Vulnerability**.
6. Click **Choose File** to locate and select the file.
7. Click **Load**.

   Data is displayed for your verification.
8. Click **Import**.

Creating an activity to remediate vulnerabilities

Use the Vulnerability Management component of IBM Data Risk Manager to view and remediate vulnerabilities. When the vulnerabilities are identified through scans, remediation actions must be taken to evaluate the correct risk exposure for the information asset.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Click **Vulnerability Management**.
4. Go to **Results View**.
5. Click **VA Data Sources**.
6. Click the filter icon under **VA Data Sources**, and select your adapter type, for example, `IBM QRadar`.
7. Alternatively, you can select a data source based on the platform.
   a) Click **VA Platforms**.
   b) Select a platform and click the database icon to select your data source.
8. For a selected data source, click the number for **Fail** to display results in the **Vulnerabilities Test Results** page.
9. Click the down arrow icon to select the severity level.
10. Click the **Remediation** icon .
11. Click **Yes** to create remediation actions.
12. On the **Create Remediation Activity** window, specify the necessary information. If the data source is from ServiceNow, you can publish the activity as an incident on ServiceNow for remediation management.
13. Click **Create**.

    On the **Vulnerabilities Test Results** page, under **Activity**, you can view activity details if the end date of activity is greater than the execution date of test results.

What to do next

You can view and manage the remediation activities that you defined in the following areas.

IBM Data Risk Manager Action Center

- Click the application menu icon .
- Click **Action Center**.

For more information about Action Center, see "Action Center" on page 140.

Asset Details window on IBM Data Risk Manager Dashboard

- Click the application menu icon .
- Click **Dashboard**.
- On the **Information Asset Portfolio** window, click the arrow icon on the asset to view the asset details.
- On the **Asset Details** window, click **Infrastructure** > **Vulnerabilities**.
- To view action items, select the infrastructure node and click **Action Items**.

Integrating IBM Security AppScan Enterprise with IBM Data Risk Manager

Application vulnerabilities for the applications that were scanned in IBM Security AppScan Enterprise can be imported into IBM Data Risk Manager. And, IBM Data Risk Manager is provisioned to trigger the vulnerability assessment scan.

IBM Data Risk Manager Integration Exchange (IntEx) agent is used to consume application vulnerabilities from IBM Security AppScan Enterprise.

For more information about installation prerequisites, see “Installation prerequisites” on page 17.

Import of application vulnerabilities from IBM Security AppScan Enterprise and triggering the vulnerability assessment scan in IBM Data Risk Manager includes the following tasks:

- Integrating IBM Security AppScan Enterprise with IBM Data Risk Manager.
- Importing IBM Security AppScan Enterprise scan templates.
- Creating application inventory in IBM Data Risk Manager.
- Importing context data.
- Creating application assessment.
- Viewing application assessment scan status.
- Viewing application assessment scan result.
- Mapping vulnerability in IBM Data Risk Manager Dashboard.
- Importing IBM Security AppScan Enterprise vulnerabilities into IBM Data Risk Manager.
- Importing endpoint vulnerabilities as CSV file into IBM Data Risk Manager.

Integrating IBM Security AppScan Enterprise with IBM Data Risk Manager

Configure IBM Data Risk Manager to communicate with IBM Security AppScan Enterprise. For the configurations steps, see “Integrating IBM Security AppScan Enterprise with IBM Data Risk Manager” on page 57.

Importing IBM Security AppScan Enterprise scan templates

Import IBM Security AppScan Enterprise scan templates into IBM Data Risk Manager. For the steps on how to import templates, see “Importing IBM Security AppScan Enterprise scan template into IBM Data Risk Manager” on page 58

Creating application inventory in IBM Data Risk Manager

Add IBM Security AppScan Enterprise data sources into IBM Data Risk Manager. For the steps on how to add data sources, see “Adding IBM Security AppScan Enterprise data sources” on page 58.

Importing context data

Import context data. Ensure that the context data is saved properly and the attributes are mapped to the appropriate inventory that was created earlier. For more information about importing context data, see “Mapping business context data” on page 99.

Note: Inventory can be created in IBM Data Risk Manager by providing the data source name and type in the context data `Database` sheet.

Creating application assessment

Use the Vulnerability Assessment component of IBM Data Risk Manager to create application assessment. For the steps on how to create application assessment, see “Creating and triggering an application assessment” on page 59.

Viewing application assessment scan status

You can view the application assessment scan status to proceed with further analysis and actions. For the steps on how to view the scan status, see Viewing scan status.

Viewing application assessment scan result

View application assessment scan results for further analysis and actions. For the steps on how to view the scan results, see Viewing scan status.

Mapping vulnerability in IBM Data Risk Manager Dashboard

When the application assessment scan is successfully completed, you can view the application vulnerability count in the Application widget on IBM Data Risk Manager Dashboard. For more information about the dashboard, see "IBM Data Risk Manager Dashboard" on page 164

Note: Count displayed is the aggregated vulnerability count inclusive of related infrastructure vulnerabilities.

Importing IBM Security AppScan Enterprise vulnerabilities into IBM Data Risk Manager

Import vulnerability scans from IBM Security AppScan Enterprise appliances into IBM Data Risk Manager inventory for data classification and risk analysis. For the steps on how to import the scan, see Importing vulnerability scans.

Note: While importing the scans, data sources and scan results are also imported.

Importing application vulnerabilities as CSV file into IBM Data Risk Manager

You can import application vulnerabilities as CSV file into IBM Data Risk Manager. For the steps on how to import the CSV file, see Importing vulnerability scans.

Remediating vulnerabilities

When the vulnerabilities are identified through scans, remediation actions must be taken to evaluate the correct risk exposure for the information asset. For the steps on how to define remediation actions, see "Creating an activity to remediate vulnerabilities" on page 45.

Integrating IBM Security AppScan Enterprise with IBM Data Risk Manager

You can configure IBM Data Risk Manager to communicate with IBM Security AppScan Enterprise to use its sensitive risk information in IBM Data Risk Manager for assessments.

About this task

The Business Context Modeler (BCM) component of IBM Data Risk Manager provides Enterprise Integration Wizard to integrate IBM Security AppScan Enterprise with IBM Data Risk Manager.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application menu icon ⋮⋮⋮.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
4. In the Adapter Configuration section, click the **Add Integration Adapter** icon ⊕.
5. Select **IBM AppScan** from the list.
6. To add an IBM Security AppScan Enterprise instance, select **IBM AppScan** from the Adapter Configuration list.

7. In the Integration Instances section, click the **Add Instance** icon ⊕.
8. Set the following options.

Option	Description
Name	Specify a name for IBM Security AppScan Enterprise instance.
URL	Specify the URL to access IBM Security AppScan Enterprise, for example `https://<appscan application-IP/host name:Port>`.
Microservice Instance	Select the agent that is needed for integration.
User Name	Specify the IBM Security AppScan Enterprise user name with administrator role.
Password	Specify the password for the user name.
AppScan Feature Key	Specify the key to establish connection with IBM Security AppScan Enterprise.
Classifier and Vulnerability Assessment	Specify the configuration file to import data from integration server to IBM Data Risk Manager for data classification and vulnerability assessments.

9. Click **Save** to save the configuration details.

What to do next

For the adapter instance that you created, you can test the connectivity. Select the instance from the **Integration Instances** list, and then click **Test Connection** to test whether the communication between IBM Security AppScan Enterprise instance and IBM Data Risk Manager server is successful.

Importing IBM Security AppScan Enterprise scan template into IBM Data Risk Manager

Import IBM Security AppScan Enterprise scan template into IBM Data Risk Manager for data analysis and assessments.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **VA Tests**.
4. To download scan templates, click the **Download** icon ⤓.
5. On the **Import** window, select an adapter instance for IBM Security AppScan Enterprise.
6. Click **Import**. When the import operation is complete, VA tests are added to the inventory.
7. To refresh VA test inventory list, click the **Refresh** icon ↻.

Adding IBM Security AppScan Enterprise data sources

You can add IBM Security AppScan Enterprise data sources into IBM Data Risk Manager inventory for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security AppScan Enterprise. For more information about integration, see "Integrating IBM Security AppScan Enterprise with IBM Data Risk Manager" on page 57.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.
4. To add IBM Security AppScan Enterprise data source, click the **Add Data Source** icon ⊕.
5. On the **Add Data Source** page, set the following options and click **Add**.

Option	Description
Server Type	Server type that you want to use. For example, **IBM Appscan**.
Data Source Name	A unique name for the data source.
Host URL	URL of the host server to import data.
IP Address	IP address of the server.
Port	Port number for connecting to the server.
Adapter	IBM Security AppScan Enterprise instance name. For example, `AppScan_Instance`.
Agents	Agent name to connect to the server.
User Name	Name of the user for connecting to the server.
Password	Password for the user name.
Encryption	Encryption status of the data source server.
Monitoring	Status of the monitoring agent.
Geographic Location	Geographic location of the data source.

   The data source that you added is listed on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **Application**.

Creating and triggering an application assessment

Use the Vulnerability Management component of IBM Data Risk Manager to create and run the assessment scan in IBM Security AppScan Enterprise to identify application vulnerabilities.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security AppScan Enterprise. For integration information, see "Integrating IBM Security AppScan Enterprise with IBM Data Risk Manager" on page 57.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Click **Vulnerability Management**.
4. Select a program from the list.
5. Click **Create New Assessment**.
6. On the **Create New Assessment** page, set the following options and click **Create Assessment**.

Option	Description
Assessment Name	IBM Security AppScan Enterprise application assessment name.
Scan Type	Scan type, for example, `Application Scanner`.
Run on	IBM Security AppScan Enterprise adapter instance to run the assessment process.

7. Under **Scope of Assessment**, add data sources to the transaction based on the scope or last scan days. Only one data source can be added to the transaction scope.
8. Click **Add Scope to Transaction**.
9. Select vulnerability test from the list and click **Save**.
10. Under **Pending Transactions** on the Transaction View, click the **Start Process** icon .
11. Select **Scan Now**.

    To schedule the scan later, select **Scan Later** and specify time to run the scan.

    To save transaction details after completion of the process under **Pending Transactions** for reuse, select **Replica**.
12. To start the process, click the **Trigger Assessment** icon .

Viewing scan status

Use the Security Command and Control Center (SC3) component of IBM Data Risk Manager to view the vulnerability assessment scan status for further analysis and actions.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the menu icon .
3. Select a program from the list.
4. Go to **Security Command and Control Center** > **Home**.
5. To view the list of completed processes along with the status, click **Vulnerability Assessment Processes**.

Viewing IBM Security AppScan Enterprise application assessment scan results

Use the Vulnerability Assessment component of IBM Data Risk Manager to view application assessment scan results for further analysis and actions.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Click **Vulnerability Management**.
4. Click **Results View**.
5. Click the filter icon under **VA Data Sources**, and select the adapter type, for example, `IBM AppScan`.
6. For the selected assessment, click the number for **Pass**, **Fail** or **Others** to display results in the **Vulnerabilities Test Results** page.

Importing vulnerability assessment scans from IBM Security AppScan Enterprise

You can import vulnerability assessment scans from IBM Security AppScan Enterprise appliances into IBM Data Risk Manager inventory for risk analysis.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security AppScan Enterprise. For more information about integration steps, see "Integrating IBM Security AppScan Enterprise with IBM Data Risk Manager" on page 57.

About this task

The transaction icon indicates that the previous import operation was successful.

The transaction icon indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Scans**.
4. Import data scans.
   a) Click the **Download** icon .
   b) On the **Import** window, select **Vulnerability Assessment**.
   c) From the **Adapter** list, select **IBM AppScan**.
   d) From the **Instances** list, select an adapter instance. You can select up to three instances.
   e) Click **Import**. When the import operation is complete, the IBM Security AppScan Enterprise vulnerability assessment scans are added to the inventory.
   f) To refresh data scan inventory list, click the **Refresh** icon .
5. To view scan results after the import operation, go to **Security Command and Control Center** > **Home**.

Importing vulnerabilities as CSV file into IBM Data Risk Manager

Use the Business Context Modeler component of IBM Data Risk Manager to import vulnerabilities as CSV file into IBM Data Risk Manager.

Before you begin

Ensure that the business context data is available for importing.

You can download the sample templates at: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**.
4. Enable the **Catalog Data** toggle button.
5. Select **Vulnerability**.

6. Click **Choose File** to locate and select the file.
7. Click **Load**.

   Data is displayed for your verification.
8. Click **Import**.

Creating an activity to remediate vulnerabilities

Use the Vulnerability Management component of IBM Data Risk Manager to view and remediate vulnerabilities. When the vulnerabilities are identified through scans, remediation actions must be taken to evaluate the correct risk exposure for the information asset.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Click **Vulnerability Management**.
4. Go to **Results View**.
5. Click **VA Data Sources**.
6. Click the filter icon under **VA Data Sources**, and select your adapter type, for example, `IBM QRadar`.
7. Alternatively, you can select a data source based on the platform.

   a) Click **VA Platforms**.

   b) Select a platform and click the database icon to select your data source.
8. For a selected data source, click the number for **Fail** to display results in the **Vulnerabilities Test Results** page.
9. Click the down arrow icon to select the severity level.
10. Click the **Remediation** icon .
11. Click **Yes** to create remediation actions.
12. On the **Create Remediation Activity** window, specify the necessary information. If the data source is from ServiceNow, you can publish the activity as an incident on ServiceNow for remediation management.
13. Click **Create**.

    On the **Vulnerabilities Test Results** page, under **Activity**, you can view activity details if the end date of activity is greater than the execution date of test results.

What to do next

You can view and manage the remediation activities that you defined in the following areas.

IBM Data Risk Manager Action Center

- Click the application menu icon .
- Click **Action Center**.

For more information about Action Center, see "Action Center" on page 140.

Asset Details window on IBM Data Risk Manager Dashboard

- Click the application menu icon .
- Click **Dashboard**.

- On the **Information Asset Portfolio** window, click the arrow icon → on the asset to view the asset details.
- On the **Asset Details** window, click **Infrastructure** > **Vulnerabilities**.
- To view action items, select the infrastructure node and click **Action Items**.

Integrating Symantec DLP with IBM Data Risk Manager

You can import the unstructured incidents that are marked as false positives in Symantec DLP into IBM Data Risk Manager. The data is then mapped to the appropriate Infrastructure in IBM Data Risk Manager.

IBM Data Risk Manager uses the following micro service for using unstructured incidents from Symantec DLP that runs on the port 8764.

```
Symantec Agent
```

For more information about installation prerequisites, see “Installation prerequisites” on page 17.

Ensure that the IBM Data Risk Manager Server image or build is available in the necessary format based on the environment where you are running the installation.

To import unstructured incidents from Symantec DLP, run the following tasks.

- IBM Data Risk Manager integration with Symantec DLP – direct link.
  - Creating incidents in Symantec DLP.
    - Discovering sensitive data.
    - Protecting sensitive data.
  - Integrating Symantec DLP with IBM Data Risk Manager.
  - Importing incidents into IBM Data Risk Manager.
  - Importing context data.
  - Mapping incidents to Infrastructure in IBM Data Risk Manager Dashboard.
  - Importing Symantec DLP policies into IBM Data Risk Manager.
- IBM Data Risk Manager integration with Symantec DLP – importing incidents through CSV file.
  - Creating Symantec DLP - unstructured inventory in IBM Data Risk Manager.
  - Importing Symantec DLP incidents as CSV file into IBM Data Risk Manager.
  - Importing context data.
  - Mapping incidents to Infrastructure in IBM Data Risk Manager Dashboard.

Discovering sensitive data

Identify the sensitive data (files) that are residing in a specific location on Windows server. Ensure that you have an SMB share on that folder.

Protecting sensitive data

1. Create policies.
   a. Create a policy group.
   b. Create a policy or multiple policies and assign to a policy group.
2. Create targets.
   a. While creating a target on the **scanned content** tab, add the content root with complete folder location.
   b. Select multiple policy groups or a single policy group.
3. Trigger Symantec DLP scan on the target to generate an incident (violation occurring on a file based on the policy).

4. Capture the incident results and save as a report which is used for further remediation. Note down the Report ID that gets displayed on the URL.

   When the incidents are saved as a report with a distinct name, the appropriate report ID is generated and displayed in the URL. Use the report ID to register Symantec DLP. You can export these incidents as a CSV file.
5. Customize report as needed based on the factors such as a specific target for which the report is needed, scan that is run on a specific date, or filter on severity.

Integrating Symantec DLP with IBM Data Risk Manager

For the integration steps, see "Integrating Symantec DLP with IBM Data Risk Manager" on page 64.

Importing incidents into IBM Data Risk Manager

For the steps on how to import incidents, see "Importing incidents from Symantec DLP" on page 65.

Importing Symantec DLP policies into IBM Data Risk Manager.

For the steps on how to import policies, see "Importing Symantec DLP policies into IBM Data Risk Manager" on page 66.

Creating Symantec DLP - unstructured inventory in IBM Data Risk Manager

For the steps on creating unstructured inventory, see "Adding Symantec DLP data sources" on page 66

Importing Symantec DLP incidents as CSV file into IBM Data Risk Manager

For the steps on importing incidents as CSV file, see "Importing Symantec DLP incidents as CSV file into IBM Data Risk Manager" on page 67.

Importing context data

Import context data. Ensure that the context data is saved properly and the attributes are mapped to the appropriate inventory that was created earlier. For more information about importing context data, see "Mapping business context data" on page 99.

Note: Inventory can be created in IBM Data Risk Manager by providing the data source name and type in the context data `Database` sheet.

Mapping incidents to Infrastructure in IBM Data Risk Manager Dashboard

1. When the Symantec DLP scans or CSV file is imported successfully, the policies that are associated with the target are available on **Newly discovered Asset** under the **Unstructured** section of Taxonomy page.
2. Apply taxonomy attributes and export the unstructured assets to dashboard.

   Note: On the Taxonomy attributes, `Application` is not applicable for `Unstructured Asset`.

Integrating Symantec DLP with IBM Data Risk Manager

You can configure IBM Data Risk Manager to communicate with Symantec Data Loss Prevention connection (DLP) for importing Symantec DLP incidents and policies into IBM Data Risk Manager.

About this task

The Business Context Modeler (BCM) component of IBM Data Risk Manager provides Enterprise Integration Wizard to integrate Symantec DLP with IBM Data Risk Manager.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.

2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
4. In the Adapter Configuration section, click the **Add Integration Adapter** icon ⊕.
5. Select **Symantec DLP** from the list.
6. To add a Symantec DLP instance, select **Symantec DLP** from the Adapter Configuration list.
7. In the Integration Instances section, click the **Add Instance** icon ⊕.
8. Set the following options.

Option	Description
Name	Specify a name for Symantec DLP instance.
URL	Specify the URL to access Symantec DLP, for example `https://<symantec application IP/host name:port>`.
Microservice Instance	Select the micro service instance that is needed for the integration.
Version of Symantec DLP	Select a Symantec DLP version for importing incidents and policies.
User Name	Specify the Symantec DLP user name with administrator role.
Password	Specify the password for the user name.
Saved Report IDs (Comma Separated)	Specify a comma-separated list of Saved Report IDs for importing the corresponding incidents reports.

9. Click **Save** to save the configuration details.

What to do next

For the adapter instance that you created, you can test the connectivity. Select the instance from the **Integration Instances** list, and then click **Test Connection** to test whether the communication between Symantec DLP instance and IBM Data Risk Manager server is successful.

Importing incidents from Symantec DLP

You can import incidents from Symantec DLP into IBM Data Risk Manager inventory for data classification and risk analysis.

Before you begin

Ensure that IBM Data Risk Manager is integrated with Symantec DLP. For more information about integration steps, see "Integrating Symantec DLP with IBM Data Risk Manager" on page 64.

About this task

The transaction icon ⇅✓ indicates that the previous import operation was successful.

The transaction icon ⇅! indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Scans**.
4. Import data scans.

   a) Click the **Download** icon .
   b) From the **Adapter** list, select **Symantec DLP**.
   c) From the **Instances** list, select an adapter instance.
   d) Click **Import** to import the scans.
   e) To refresh scan inventory list, click the **Refresh** icon .
5. To view scan results after the import operation, go to **Security Command and Control Center** > **Home**.

Importing Symantec DLP policies into IBM Data Risk Manager

You can import Symantec DLP policies into IBM Data Risk Manager inventory for data classification and risk analysis.

About this task

The transaction icon indicates that the previous import operation was successful.

The transaction icon indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Policies**.
4. Import policies.
   a) Click the **Download** icon .
   b) On the **Import** window, select a Symantec DLP instance from the **Instances** list.
   c) Click **Choose Files** to select the XML file.

      Note: In Symantec DLP, export the policies into an XML file.

      When the policies are loaded successfully, you can view the policies in **Policy Management** > **Cleansing Policies** > **Unstructured**. You can use these policies to trigger the unstructured native scan.

Adding Symantec DLP data sources

You can add Symantec DLP data sources into IBM Data Risk Manager inventory for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with Symantec DLP. For more information about integration, see "Integrating Symantec DLP with IBM Data Risk Manager" on page 64.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.

4. To add a Symantec DLP data source, click the **Add Data Source** icon ⊕.
5. On the **Add Data Source** page, set the following options and click **Add**.

Option	**Description**
Server Type	Data source server type that you want to use. For example, **IDRM**.
Target	Name for the data source.
IP Address	IP address of the data source server.
Port	Port number for connecting to the server.
Port Type	File sharing protocol to access data.
Target Path	Target path to import unstructured data.
Adapter	Symantec DLP instance name. For example, `Symantec DLP Instance`.
Agents	Agent name to connect to the data source.
User Name	Name of the user.
Password	Password for the user name.
Encryption	Encryption status of the data source server.
Monitoring	Status of monitoring agent data source server.
Geographic Location	Geographic location of the data source.

   The data source that you added is listed on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **File Storage**.

Importing Symantec DLP incidents as CSV file into IBM Data Risk Manager

You can import Symantec DLP incidents into IBM Data Risk Manager inventory for data classification and risk analysis.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**.
4. Enable the **Catalog Data** toggle button.
5. Click the **Incidents** tab.
6. Click **Choose File** to locate and select the file.
7. Click **Load**.

   Data is displayed for your verification.
8. Click **Import**.

   Note: Ensure that the inventory is created in IBM Data Risk Manager before you upload the CSV file.

Integrating ServiceNow with IBM Data Risk Manager

You must configure ServiceNow to import configuration management database (CMDB) data into IBM Data Risk Manager and use this data along with applications and business context. You can also publish activities that are created in Action Center to ServiceNow for remediation activities.

IBM Data Risk Manager uses the following micro service for using application vulnerabilities from ServiceNow that runs on the port 8787.

```
ServiceNow (Consuming the CMDB Data) – runs on port 8787
```

For more information on prerequisites, see "Installation prerequisites" on page 17.

Ensure that the IBM Data Risk Manager Server image or build is available in the necessary format based on the environment where you are running the installation.

To import ServiceNow CMDB data into IBM Data Risk Manager, run the following tasks.

- Integrating ServiceNow with IBM Data Risk Manager.
- Importing ServiceNow CMDB data into IBM Data Risk Manager.
- ServiceNow entity mapping with IBM Data Risk Manager

Integrating ServiceNow with IBM Data Risk Manager

For the integration steps, see "Integrating ServiceNow with IBM Data Risk Manager" on page 69.

Importing ServiceNow CMDB data into IBM Data Risk Manager

For the steps on how to import, see "Importing ServiceNow CMDB into IBM Data Risk Manager" on page 70.

ServiceNow entity mapping with IBM Data Risk Manager

You must use basic authentication mode to connect to ServiceNow. Following table illustrates the key mapping between ServiceNow entities and IBM Data Risk Manager.

ServiceNow Entity	Mapping Entity
cmdb_ci_business_app	Application
cmdb_ci_service	Application
cmdb_ci_appl	Application
cmdb_ci_business_process	Business Process
cmdb_ci_database	Inventory
cmdb_ci_app_server	Inventory
cmdb_ci_db_instance	Inventory
cmdb_ci_server	Inventory
cmdb_ci_ip_address	Internally used to map IP address for the Inventory by using `cmdb_rel_ci` Object.
cmn_department	Used for resolving department list of values.
cmdb_rel_ci	Entity relationship object that is used to establish the relationship across entities.
cmn_cost_center	Used for resolving department list of values
cmdb_rel_type	Master list of Relationship type

sys_user	Master list of Resources and User
cmn_location	Used for resolving location list of values
core_company	Used for resolving company list of values

When the CMDB data is imported into IBM Data Risk Manager, based on the entity mapping, context data resolution and tagging happens automatically. Now, the inventories that are sourced from ServiceNow can be managed appropriately (Database, File Storage, Application, and Server) on **Business Context Modeler** > **Manage Inventory**.

Publishing activities on ServiceNow for remediation management

For a ServiceNow data source, you can create an activity in Action Center and publish it as an incident on ServiceNow for remediation management. Currently, you can publish the activity only on a single instance of ServiceNow. For more information about Action Center, see "Action Center" on page 140.

Integrating ServiceNow with IBM Data Risk Manager

You must configure IBM Data Risk Manager to connect and interact with ServiceNow for importing configuration management database (CMDB) data into IBM Data Risk Manager and use this data along with applications and business context.

About this task

The Business Context Modeler (BCM) component of IBM Data Risk Manager provides Enterprise Integration Wizard to integrate ServiceNow with IBM Data Risk Manager.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
4. In the Adapter Configuration section, click the **Add Integration Adapter** icon ⊕.
5. Select **ServiceNow** from the list.
6. To add a ServiceNow instance, select **ServiceNow** from the Adapter Configuration list.
7. In the Integration Instances section, click the **Add Instance** icon ⊕.
8. Set the following options.

Option	Description
Name	Specify a name for ServiceNow instance.
URL	Specify the URL to access ServiceNow, for example `https://<servicenow application-IP/host name:port>`.
Microservice Instance	Select the micro service instance that is needed for the integration.
User Name	Specify the ServiceNow user name with administrator role.
Password	Specify the password for the user name.
Enable OAth Authentication	Select to enable OAth authentication.
ServiceNow Client Secret Key	Specify the secret key.
ServiceNow Client ID	Specify the client ID.

9. Click **Save** to save the configuration details.

What to do next

For the adapter instance that you created, you can test the connectivity. Select the instance from the **Integration Instances** list, and then click **Test Connection** to test whether the communication between ServiceNow instance and IBM Data Risk Manager server is successful.

Importing ServiceNow CMDB into IBM Data Risk Manager

Use the Business Context Modeler component of IBM Data Risk Manager to import ServiceNow configuration management database (CMDB) data into IBM Data Risk Manager.

Before you begin

Ensure that IBM Data Risk Manager is integrated with ServiceNow. For integration information, see "Integrating ServiceNow with IBM Data Risk Manager" on page 69.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**.
4. Click **Load from ServiceNow**.
5. Click **Refresh**.
6. Click **Yes** to refresh the data from ServiceNow.

Integrating IBM InfoSphere Information Governance Catalog with IBM Data Risk Manager

Configure IBM Data Risk Manager to communicate with IBM InfoSphere Information Governance Catalog (IGC) for receiving assets that are defined in the IGC catalog. Integration provides a holistic representation of the assets that govern information in the catalog.

IBM Data Risk Manager uses the following micro service to consume assets that are defined in the IGC catalog.

```
IGC (IGC agent)  – runs on port 8768
```

Prerequisites

Ensure that you have the IBM Data Risk Manager Server image or build in the necessary format based on the environment where you are running the installation.

- Recommended version of IGC for integration is 11.7.
- Assets must be associated with only structured data.
- In the IGC catalog, relationship between application and assets entity is not necessary.
- Following attributes must be defined for the assets of type `Database` in the IGC catalog that are currently supported for import into IBM Data Risk Manager.
  - `modified_on`
  - `short_description`
  - `dbms_server_instance`
  - `name`
  - `dbms_version`
  - `dbmsv`
  - `created_by`

  - `dbms_vendor`
  - `created_on`
  - `modified_by`
  - `location`
- Assets that are imported from IGC catalog must be mutually exclusive or identical to the assets that are loaded through other flat files such as CMDB reports by using the IBM Data Risk Manager Business Context Modeling component.

Workflow

- After IGC integration configuration in IBM Data Risk Manager, import assets that are defined in the IGC catalog.
- Assets that are imported by using the `label` attribute must be defined for all terms that are planned for import.
- Terms must be categorized in IGC based on a selected taxonomy.
  - All the terms that are logically related must be grouped by using IGC Categories.
  - Set the **Referencing Categories** field with appropriate Category for the respective term.
- All the terms must be assigned assets, and only those assets are imported.
- Workflow: **Labels** > **Assets (Columns)** > **Database Details**, for example, **schemas**.

Integrating IGC with IBM Data Risk Manager

Configure IBM Data Risk Manager to communicate with IGC. For the configurations steps, see "Integrating IBM InfoSphere Information Governance Catalog with IBM Data Risk Manager" on page 72.

Importing assets defined in the IGC catalog

Import the assets that are defined in IGC catalog. For the steps on how to import, see "Importing assets defined in IBM InfoSphere Information Governance Catalog" on page 73.

Exporting tagged assets to taxonomy

Export tagged assets for taxonomy assignment and publishing. For the steps on how to export, see "Exporting tagged assets to taxonomy" on page 74.

Importing context data

You can import the business context data into IBM Data Risk Manager by using one or multiple files in comma-separated values (CSV) format.

1. Ensure that the database, application, and business process sheets are edited for assets that are defined in the IGC catalog.
2. Import the context data sheet.
3. Ensure that the context data is saved properly and attributes are mapped to the appropriate inventory for which the tables are tagged in **Security Command and Control Center** > **Analysis** > **Analysis Workbench**.

For more information about mapping business context data, see "Mapping business context data" on page 99.

Exporting data assets to IBM Data Risk Manager Dashboard

For the steps on how to export assets to the dashboard, see "Taxonomy mapping" on page 136.

Validating information assets in IBM Data Risk Manager Dashboard

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the menu icon ⠿.
3. Click **Dashboard**.
4. Select the appropriate information asset.
5. Validate details for **Infrastructure**, **Stakeholders**, **Processes**, and **Application**.
6. Click the **Asset Details** icon → to validate the mapped IGC attributes.

For more information about IBM Data Risk Manager Dashboard, see "IBM Data Risk Manager Dashboard" on page 164.

Integrating IBM InfoSphere Information Governance Catalog with IBM Data Risk Manager

Configure IBM Data Risk Manager to communicate with IBM InfoSphere Information Governance Catalog for importing metadata into IBM Data Risk Manager.

About this task

The Business Context Modeler (BCM) component of IBM Data Risk Manager provides Enterprise Integration Wizard to integrate IBM InfoSphere Information Governance Catalog with IBM Data Risk Manager.

Kafka is a message queue to get live notifications from IBM InfoSphere Information Governance Catalog and IBM Data Risk Manager. In this queue, IBM InfoSphere Information Governance Catalog is the Producer and IBM Data Risk Manager is the Consumer. You can configure IBM Data Risk Manager to subscribe to the IBM InfoSphere Information Governance Catalog topics and receive notifications regularly for processing the messages.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
4. In the Adapter Configuration section, click the **Add Integration Adapter** icon ⊕.
5. Select **IBM Information Governance Catalog** from the list.
6. To add an IBM InfoSphere Information Governance Catalog instance, select **IBM Information Governance Catalog** from the Adapter Configuration list.
7. In the Integration Instances section, click the **Add Instance** icon ⊕.
8. Set the following options.

Option	Description
Name	Specify a name for IBM InfoSphere Information Governance Catalog instance.
URL	Specify the URL to access IBM InfoSphere Information Governance Catalog, for example `https://<information governance catalog application-IP/host name:Port>`.
Microservice Instance	Select the micro service instance that is needed for the integration.
Versions of IGC	Select a IBM InfoSphere Information Governance Catalog version for importing metadata.

Option	Description
User Name	Specify the IBM InfoSphere Information Governance Catalog user name with administrator role.
Password	Specify the password for the user name.

9. To configure IBM Data Risk Manager to subscribe to the IBM InfoSphere Information Governance Catalog topics and receive notifications regularly for processing messages, click **Kafka Configuration**, and then specify the configuration information.

Option	Description
Bootstrap Server	Specify the host or port details to use for establishing the initial connection to the Kafka server.
IGC Topic	Specify the name of the Kafka topic where messages are published.
Group ID	Specify the group ID to publish messages when multiple Kafka consumer nodes are used.
User Name	Specify the user name to authenticate with the Kafka server.
Password	Specify the password for the user name.
Mark for Delete	Select to delete or remove the Kafka server configuration.

10. Click **Save** to save the configuration details.

What to do next

For the adapter instance that you created, you can test the connectivity. Select the instance from the **Integration Instances** list, and then click **Test Connection** to test whether the communication between IBM InfoSphere Information Governance Catalog instance and IBM Data Risk Manager server is successful.

Importing assets defined in IBM InfoSphere Information Governance Catalog

You can import catalog data (assets) that are defined in IBM InfoSphere Information Governance Catalog (IGC) catalog into IBM Data Risk Manager inventory for risk analysis.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IGC. For integration information, see "Integrating IBM InfoSphere Information Governance Catalog with IBM Data Risk Manager" on page 72.

Procedure

1. Identify sensitive data assets along with terms in IGC (catalog) and assign labels.
2. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
3. Click the application menu icon.
4. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Scans**.
5. Import assets.
   a) Click the **Download** icon.
   b) From the **Adapter** list, select **Information Governance Catalog**
   c) From the **Instances** list, select an adapter instance.
6. Select IGC micro service name, label, and category from the respective drop-down lists for structured and unstructured data.
7. Click **Import**.

Exporting tagged assets to taxonomy

Export the tagged assets for taxonomy assignment and publishing.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the menu icon ⠿.
3. Go to **Security Command and Control Center** > **Analysis**.
4. Select the appropriate database that is relevant to IBM InfoSphere Information Governance Catalog.
5. Validate the tagged tables.
6. To export the filtered set of data elements, click the **Export to Taxonomy** icon.
7. When prompted, click **Yes** to export the data sets to taxonomy.
8. Click the **Exported** icon 245 to view the exported tables.

What to do next

Go to **Security Command and Control Center** > **Taxonomy** to validate whether the export operation is successful.

Integrating Imperva SecureSphere with IBM Data Risk Manager

Configure IBM Data Risk Manager to connect and interact with Imperva SecureSphere for importing vulnerability information into IBM Data Risk Manager.

IBM Data Risk Manager uses Fullstack to consume the vulnerabilities from Imperva SecureSphere.

Ensure that the IBM Data Risk Manager Server image or build is available in the necessary format based on the environment where you are running the installation.

To import Imperva SecureSphere vulnerability data into IBM Data Risk Manager, run the following tasks.

- Importing Imperva SecureSphere vulnerability assessment into IBM Data Risk Manager.
  - Assessment
  - Integrating Imperva SecureSphere with IBM Data Risk Manager.
  - Importing vulnerability assessment tests.
  - Importing vulnerabilities into IBM Data Risk Manager.
  - Importing vulnerabilities as CSV file into IBM Data Risk Manager.
- Importing Imperva SecureSphere classification scan results into IBM Data Risk Manager.
  - Imperva SecureSphere discovery and classification.
  - Importing Imperva SecureSphere classifier results into IBM Data Risk Manager through native catalog.

Assessment

The Secure Sphere Assessment Server enables you to import scans from third-party vendors such as IBM AppScan, HP Web Inspect, NTObjectives, ImmuniWeb, acunetix, and White Hat for listing vulnerabilities in the Secure Sphere vulnerability workbench. Secure Sphere integrates Common Vulnerabilities Scoring System (CVSS) that is maintained by National Institute of Standards and Technology. The scoring system scores each vulnerability on a scale of 0 to 10 based on the effect that the vulnerability has, and the effort that is required to use it.

Integrating Imperva SecureSphere with IBM Data Risk Manager

For the integration steps, see “Integrating Imperva SecureSphere with IBM Data Risk Manager” on page 75.

Importing Imperva SecureSphere vulnerability assessments (VA) tests

For the steps on how to import VA tests, see “Importing Imperva SecureSphere vulnerability assessment tests” on page 76.

Importing Imperva SecureSphere vulnerabilities into IBM Data Risk Manager

For the steps on how to import vulnerabilities, see Importing vulnerability scans.

Importing Imperva SecureSphere vulnerabilities as CSV file into IBM Data Risk Manager

You can import vulnerabilities as CSV file into IBM Data Risk Manager. For the steps on how to import the CSV file, see Importing vulnerability scans.

Secure Sphere Discovery and Classification

Secure Sphere Discovery and Classification provides a complete set of tools to help you discover web services. You then use this classification information to create security policies to monitor them and alert you about the suspicious activities.

The Discovery and Classification window provides a wide selection of options that enable you to navigate between the available features to configure scans and display discovered server.

You can trigger the classification scan in Imperva SecureSphere and the results can be exported to a CSV file. These contents can be customized by using the IBM Data Risk Manager native catalog classifier template and can be imported into IBM Data Risk Manager.

Importing Imperva SecureSphere classifier results into IBM Data Risk Manager

For the steps on how to import classifier results CSV file (Catalog data) into IBM Data Risk Manager, see “Importing classifier results CSV file (catalog data) into IBM Data Risk Manager” on page 40.

Integrating Imperva SecureSphere with IBM Data Risk Manager

You must configure IBM Data Risk Manager to connect and interact with Imperva SecureSphere for importing vulnerability information into IBM Data Risk Manager.

About this task

The Business Context Modeler (BCM) component of IBM Data Risk Manager provides Enterprise Integration Wizard to integrate Imperva SecureSphere with IBM Data Risk Manager.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
4. In the Adapter Configuration section, click the **Add Integration Adapter** icon ⊕.
5. Select **Imperva** from the list.
6. To add an Imperva SecureSphere instance, select **Imperva** from the Adapter Configuration list.
7. In the Integration Instances section, click the **Add Instance** icon ⊕.
8. Set the following options.

Option	Description
Name	Specify a name for Imperva SecureSphere instance.
URL	Specify the URL to access Imperva SecureSphere, for example `https://<imperva application-IP/host name:port>`.
User Name	Specify the Imperva SecureSphere user name with administrator role.
Password	Specify the password for the user name.

9. Click **Save** to save the configuration details.

Importing Imperva SecureSphere vulnerability assessment tests

Import Imperva SecureSphere vulnerability assessment (VA) tests into IBM Data Risk Manager for analysis.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application navigation icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **VA Tests**.
4. To download scan templates, click the download icon .
5. On the **Import** window, select the adapter instance for Imperva SecureSphere.
6. Click **Import**. When the import operation is complete, VA tests are added to the inventory.
7. To refresh VA test inventory list, click the **Refresh** icon .

Importing Imperva SecureSphere vulnerabilities into IBM Data Risk Manager

You can import vulnerability scans from Imperva SecureSphere appliances into IBM Data Risk Manager inventory for risk analysis.

Before you begin

When the scans are imported, scan results are also imported. Ensure that you import the sites from Imperva SecureSphere first.

About this task

The transaction icon indicates that the previous import operation was successful.

The transaction icon indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Scans**.
4. Import data scans.

   a) Click the **Download** icon .

   b) On the **Import** window, select **Vulnerability Assessment**.

   c) From the **Adapter** list, select **Imperva**.

- d) From the **Adapters** list, select an adapter instance. You can select up to three instances.
- e) Select the date from which you need to pull vulnerability scans from Imperva SecureSphere.
- f) Click **Import**. When the import operation is complete, the Imperva SecureSphere vulnerability scans are added to the inventory.
- g) To refresh data scan inventory list, click the **Refresh** icon ⟳.

5. To view the scan results after the import operation, go to **Security Command and Control Center** > **Home**.

Importing vulnerabilities as CSV file into IBM Data Risk Manager

Use the Business Context Modeler component of IBM Data Risk Manager to import vulnerabilities as CSV file into IBM Data Risk Manager.

Before you begin

Ensure that the business context data is available for importing.

You can download the sample templates at: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**.
4. Enable the **Catalog Data** toggle button.
5. Select **Vulnerability**.
6. Click **Choose File** to locate and select the file.
7. Click **Load**.

   Data is displayed for your verification.
8. Click **Import**.

Importing classifier results CSV file (catalog data) into IBM Data Risk Manager

Use the Business Context Modeler component of IBM Data Risk Manager to import classifier results as CSV file into IBM Data Risk Manager.

Before you begin

Ensure that the business context data is available for importing.

You can download the sample templates at: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**.
4. Enable the **Catalog Data** toggle button.
5. Select **Classification**.
6. Click **Choose File** to locate and select the file.
7. Click **Load**.

Data is displayed for your verification.

8. Click **Import**.

Integrating IBM Multi-Cloud Data Encryption with IBM Data Risk Manager

Configure IBM Data Risk Manager to connect and interact with IBM Multi-Cloud Data Encryption to fetch encryption details of data sources that are added to the inventory from various sources where IBM Multi-Cloud Data Encryption agent is deployed for data encryption.

Ensure that the IBM Data Risk Manager Server image or build is available in the necessary format based on the environment where you are running the installation.

To fetch and view encryption status of data sources in IBM Data Risk Manager, run the following tasks.

Integrating IBM Multi-Cloud Data Encryption with IBM Data Risk Manager

For the integration steps, see "Integrating IBM Multi-Cloud Data Encryption with IBM Data Risk Manager" on page 78.

Fetching IBM Multi-Cloud Data Encryption status

For the steps on how to fetch data source encryption details, see "Fetching IBM Multi-Cloud Data Encryption status of data sources" on page 79.

Viewing IBM Multi-Cloud Data Encryption encryption status on dashboard

You can view encryption status of the data sources that you fetched from IBM Multi-Cloud Data Encryption on the **Infrastructure** widget of IBM Data Risk Manager Dashboard. For the steps on how to view the status on dashboard, see "Viewing IBM Multi-Cloud Data Encryption encryption status on dashboard" on page 79.

Integrating IBM Multi-Cloud Data Encryption with IBM Data Risk Manager

You must configure IBM Data Risk Manager to connect and interact with IBM Multi-Cloud Data Encryption to fetch encryption details of data sources that are added to the inventory from various sources where IBM Multi-Cloud Data Encryption agent is deployed for data encryption.

About this task

The Business Context Modeler (BCM) component of IBM Data Risk Manager provides Enterprise Integration Wizard to integrate IBM Multi-Cloud Data Encryption with IBM Data Risk Manager.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
4. In the Integration Platforms section, click the **Add Integration Adapter** icon ⊕.
5. Select **IBM MDE** from the list.
6. To add an IBM Multi-Cloud Data Encryption instance, select **IBM MDE** from the Integration Platforms list.
7. In the Integration Instances section, click the **Add Instance** icon ⊕.
8. Set the following options.

Option	Description
Name	Specify IBM Multi-Cloud Data Encryption instance name.

Option	Description
URL	Specify the URL to access IBM Multi-Cloud Data Encryption, for example `https://<MDE server -IP/host name:port>`.
Microservice Instance	Select the micro service instance that is needed for the integration.
User Name	Specify the IBM Multi-Cloud Data Encryption user name with administrator role.
Password	Specify the password for the user name.
Classifier and Vulnerability Assessment	Specify the configuration file to import data from integration server to IBM Data Risk Manager for data classification and vulnerability assessments.

9. Click **Save** to save the configuration details.

What to do next

For the adapter instance that you created, you can test the connectivity. Select the instance from the **Integration Instances** list, and then click **Test Connection** to test whether the communication between IBM Multi-Cloud Data Encryption instance and IBM Data Risk Manager server is successful.

Fetching IBM Multi-Cloud Data Encryption status of data sources

Fetch IBM Multi-Cloud Data Encryption status of data sources to view them on IBM Data Risk Manager data source inventory.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application navigation icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory**.
4. Click **Sync Monitoring Status**.
5. Select IBM Multi-Cloud Data Encryption adapter from the **Adapters** list.
6. Click **Refresh**.

   In the Manage Inventory window, if encryption is active for the data sources from the adapter that you specified, the **Encryption Active** 🔒 icon is displayed.

Viewing IBM Multi-Cloud Data Encryption encryption status on dashboard

You can view encryption status of the data sources that you fetched from IBM Multi-Cloud Data Encryption on the **Infrastructure** widget of IBM Data Risk Manager Dashboard.

Before you begin

Ensure that IBM Multi-Cloud Data Encryption is integrated with IBM Data Risk Manager to get encryption status. For the integration steps, see "Integrating IBM Multi-Cloud Data Encryption with IBM Data Risk Manager" on page 78.

Procedure

1. Log in to IBM Data Risk Manager Application Suite by using your credentials.
2. Click the menu icon ⠿.
3. Click **Dashboard**. The **Information Asset Portfolio** page displayed.
4. Click an information asset to display the dashboard widgets.
5. On the **Infrastructure** widget, you can view icon 🔒 that indicates whether the encryption status is active.

Integrating OneTrust with IBM Data Risk Manager

Configure IBM Data Risk Manager to connect and interact with OneTrust to import inventories and their corresponding risk information into IBM Data Risk Manager. These risks are mapped to the appropriate information assets and infrastructure in IBM Data Risk Manager to view them on the dashboard for risk analysis and actions.

Ensure that the IBM Data Risk Manager Server image or build is available in the necessary format based on the environment where you are running the installation.

You can import the following types of inventory from OneTrust.

- Assets
  - Application
  - Database
  - Physical Storage
  - Website
  - Vendor
- Processing Activities
- Vendors

To import inventory list and risk details from OneTrust into IBM Data Risk Manager, run the following tasks.

Integrating OneTrust with IBM Data Risk Manager

For the integration steps, see "Integrating OneTrust with IBM Data Risk Manager" on page 80.

Importing inventories and risk information from OneTrust

For more information about how to import inventories, see "Importing OneTrust inventories and risk information" on page 81.

Viewing OneTrust inventories and risk information on a splash widget

For more information about how to view risk information, see "Viewing OneTrust inventories and risk information on a splash widget" on page 81.

Integrating OneTrust with IBM Data Risk Manager

Configure IBM Data Risk Manager to connect and interact with OneTrust to import inventories and their corresponding risk information into IBM Data Risk Manager.

About this task

The Business Context Modeler (BCM) component of IBM Data Risk Manager provides Enterprise Integration Wizard to integrate OneTrust with IBM Data Risk Manager.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with your user credentials.
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
4. In the Integration Platforms section, click the **Add Integration Adapter** icon ⊕.
5. Select **OneTrust** from the list.
6. To add an OneTrust instance, select **OneTrust** from the Integration Platforms list.

7. In the Integration Instances section, click the **Add Instance** icon ⊕.
8. Set the following options.

Option	Description
Name	Specify OneTrust instance name.
URL	Specify the URL to access OneTrust, for example, `https:/example.com/`.
Microservice Instance	Select the integration agent from the list.
API Key	Specify the API key to import data by using the HTTP API of OneTrust. API keys are used to authenticate your HTTP API requests.
Classifier and Vulnerability Assessment	Specify the configuration file to import data from integration server to IBM Data Risk Manager for data classification and vulnerability assessments.

9. Click **Save** to save the configuration details.

What to do next

For the adapter instance that you created, you can test the connectivity. Select the instance from the **Integration Instances** list, and then click **Test Connection** to test whether the communication between OneTrust instance and IBM Data Risk Manager server is successful.

Importing OneTrust inventories and risk information

Import OneTrust inventories and risk information into IBM Data Risk Manager for risk analysis and actions.

Procedure

1. Log in to IBM Data Risk Manager Application Suite by using your credentials.
2. Click the application navigation icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Risk**.
4. Click the import icon .
5. On the **Import** window, select an appropriate OneTrust adapter instance.
6. Click **Import**.

   The inventory list and the corresponding risk information from OneTrust are displayed on the **Risk Assessment** page.

Viewing OneTrust inventories and risk information on a splash widget

You can view data that you imported from OneTrust on the Information Asset Distribution widget of IBM Data Risk Manager Privacy Splash page to quickly visualize and analyze risk information.

Procedure

1. Log in to IBM Data Risk Manager Application Suite by using your credentials.
2. Click the menu icon ⠿.
3. Click **Privacy Splash**.
4. On the **Information Asset Distribution** > **Privacy Risk** widget, you can view the risk information in detail.

Integrating IBM Security Guardium Analyzer with IBM Data Risk Manager

Configure IBM Data Risk Manager to connect and interact with IBM Security Guardium Analyzer for importing classifier scans and vulnerability information into IBM Data Risk Manager.

Ensure that the IBM Data Risk Manager Server image or build is available in the necessary format based on the environment where you are running the installation.

To import data from IBM Security Guardium Analyzer into IBM Data Risk Manager for risk analysis, run the following tasks.

Importing data sources from IBM Security Guardium Analyzer

For more information about how to import data sources, see “Importing IBM Security Guardium Analyzer data sources” on page 83.

Integrating IBM Security Guardium Analyzer with IBM Data Risk Manager

For the integration steps, see “Integrating IBM Security Guardium Analyzer with IBM Data Risk Manager” on page 82.

Importing classifier scans from IBM Security Guardium Analyzer

For more information about how to import classifier scans, see “Importing classifier scans from IBM Security Guardium Analyzer” on page 84.

Importing vulnerability scans from IBM Security Guardium Analyzer

For more information about how to import vulnerability scans, see “Importing IBM Security Guardium Analyzer vulnerability scans into IBM Data Risk Manager” on page 84.

Viewing vulnerability assessment scan results

For more information about how to view vulnerability assessment scan results, see “Viewing vulnerability assessment scan results for IBM Security Guardium Analyzer” on page 85.

Mapping vulnerabilities from IBM Security Guardium Analyzer on IBM Data Risk Manager Dashboard

Click the Information Asset Portfolio secondary page of dashboard to view the IBM Security Guardium Analyzer vulnerabilities on the **Vulnerabilities** tab. For more information about the dashboard, see “IBM Data Risk Manager Dashboard” on page 164.

Integrating IBM Security Guardium Analyzer with IBM Data Risk Manager

Configure IBM Data Risk Manager to connect and interact with IBM Security Guardium Analyzer to import classifier scans and vulnerability assessment scans into IBM Data Risk Manager.

About this task

The Business Context Modeler (BCM) component of IBM Data Risk Manager provides Enterprise Integration Wizard to integrate IBM Security Guardium Analyzer with IBM Data Risk Manager.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with your user credentials.
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
4. In the Adapter Configuration section, click the **Add Integration Adapter** icon ⊕.
5. Select **IBM Guardium Analyzer** from the list.

6. To add an IBM Security Guardium Analyzer instance, select **IBM Guardium Analyzer** from the Adapter Configuration list.
7. In the Integration Instances section, click the **Add Instance** icon ⊕.
8. Set the following options.

Option	Description
Name	Specify IBM Security Guardium Analyzer instance name.
URL	Specify the URL to access IBM Security Guardium Analyzer. for example, `https://www.example.com/`.
Microservice Instance	Select integration agent from the list.
User Name	Specify the IBM Security Guardium Analyzer user name.
Password	Specify password for the user name.
Classifier and Vulnerability Assessment	Specify the configuration file to import data from integration server to IBM Data Risk Manager for data classification and vulnerability assessments.

9. Click **Save** to save the configuration details.

What to do next

For the adapter instance that you created, you can test the connectivity. Select the instance from the **Integration Instances** list, and then click **Test Connection** to test whether the communication between IBM Security Guardium Analyzer instance and IBM Data Risk Manager server is successful.

Importing IBM Security Guardium Analyzer data sources

You can import data sources from IBM Security Guardium Analyzer into IBM Data Risk Manager inventory for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security Guardium Analyzer. For more information about integration, see "Integrating IBM Security Guardium Analyzer with IBM Data Risk Manager" on page 82.

About this task

The transaction icon ✓ indicates that the previous import operation was successful.

The transaction icon ! indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Source**.
4. Import data sources.

   a) Click the **Download** icon ⤓.

   b) On the **Import** window, select an IBM Security Guardium Analyzer instance.

   c) Click **Import**.

When the import operation is complete, the IBM Security Guardium Analyzer data sources are added to the inventory.

d) To refresh data source inventory list, click the **Refresh** icon ⟳.

The data source that you added is listed on the **Data Source** page. Alternatively, you can also view the data sources that you imported on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **Database**.

Importing classifier scans from IBM Security Guardium Analyzer

You can import classifier scans from IBM Security Guardium Analyzer into IBM Data Risk Manager inventory for risk analysis.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security Guardium Analyzer. For more information about the integration, see "Integrating IBM Security Guardium Analyzer with IBM Data Risk Manager" on page 82.

About this task

The transaction icon ✓ indicates that the previous import operation was successful.

The transaction icon ! indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Scans**.
4. Import data scans.

   a) Click the **Download** icon ⤓.

   b) On the **Import** window, select **Classifier**.

   c) From the **Adapter** list, select **IBM Guardium Analyzer**.

   d) From the **Instances** list, select an adapter instance. You can select up to three instances.

   e) Click **Import**. When the import operation is complete, the IBM Security Guardium Analyzer classifier scans are added to the inventory.

   f) To refresh data scan inventory list, click the **Refresh** icon ⟳.
5. Alternatively, to view scan results after the import operation, go to **Security Command and Control Center** > **Home**.

Importing IBM Security Guardium Analyzer vulnerability scans into IBM Data Risk Manager

You can import vulnerability scans from IBM Security Guardium Analyzer into IBM Data Risk Manager inventory for risk analysis.

About this task

The transaction icon ✓ indicates that the previous import operation was successful.

The transaction icon ! indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Scans**.
4. Import data scans.

   a) Click the **Download** icon .

   b) On the **Import** window, select **Vulnerability Assessment**.

   c) From the **Adapter** list, select **IBM Guardium Analyzer**.

   d) From the **Instances** list, select an adapter instance. You can select up to three instances.

   e) Click **Import**. When the import operation is complete, the IBM Security Guardium Analyzer vulnerability assessment scans are added to the inventory.

   f) To refresh data scan inventory list, click the **Refresh** icon .
5. Alternatively, to view scan results after the import operation, go to **Security Command and Control Center** > **Home**.

Viewing vulnerability assessment scan results for IBM Security Guardium Analyzer
Use the Vulnerability Assessment component of IBM Data Risk Manager to view vulnerability assessment scan results for further analysis and actions.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Click **Vulnerability Management**.
4. Click **Results View**.
5. Click the filter icon under **VA Data Sources**, and select the adapter type, for example, `IBM Guardium Analyzer`.
6. For the selected assessment, click the number for **Pass**, **Fail**, or **Others** to display results in the **Vulnerabilities Test Results** page.
7. To view results based on the database platform, click **VA Platforms**.

Integrating IBM StoredIQ with IBM Data Risk Manager

Configure IBM Data Risk Manager to connect and interact with IBM StoredIQ to use its classification data results for risk analysis and actions. IBM StoredIQ provides scalable analysis and governance of unstructured data in-place across disparate and distributed email, file shares, desktops, and collaboration sites.

A volume represents a data source or destination that is available on the network to IBM StoredIQ. An infoset can contain multiple volumes. Infoset is the core concept in using the IBM StoredIQ applications. It is created and used to collect specific data to manage the business system. The reporting function provides external views of infoset and validates IBM StoredIQ processes. You can share the information that is contained within infoset with the reporting component, which allows infoset to be transferred to other media types for review and analysis. Currently, you can import only the **CSV Term Hit Details Export** report into IBM Data Risk Manager for data analysis.

For more information about IBM StoredIQ, see the product documentation at: https://www.ibm.com/support/knowledgecenter/SSSHEC_7.6.0/welcome/storediq.html

To import data from IBM StoredIQ into IBM Data Risk Manager, run the following tasks.

Integrating IBM StoredIQ with IBM Data Risk Manager

For the integration steps, see "Integrating IBM StoredIQ with IBM Data Risk Manager" on page 86.

Importing data sources from IBM StoredIQ

For more information about how to import data sources, see "Importing IBM StoredIQ data sources" on page 87.

Importing classifier scans from IBM StoredIQ

For more information about how to import classifier scans, see "Importing classifier scans from IBM StoredIQ" on page 87.

Mapping the classification results data to Infrastructure in IBM Data Risk Manager Dashboard

1. When the IBM StoredIQ scans are imported successfully, the assets that are associated with the data source are available on **Security Command and Control Center** > **Taxonomy** > **Unstructured** > **Newly Discovered Assets**. Select the assets.
2. Apply appropriate primary and secondary attributes.
3. Export the unstructured information assets to IBM Data Risk Manager Dashboard.
4. Corresponding classifier results are mapped to the appropriate infrastructure in IBM Data Risk Manager Dashboard.

Integrating IBM StoredIQ with IBM Data Risk Manager

Configure IBM Data Risk Manager to connect and interact with IBM StoredIQ to use its classification data results for risk analysis and actions.

About this task

The Business Context Modeler (BCM) component of IBM Data Risk Manager provides Enterprise Integration Wizard to integrate IBM StoredIQ with IBM Data Risk Manager.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with your user credentials.
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
4. In the Adapter Configuration section, click the **Add Integration Adapter** icon ⊕.
5. Select **Stored IQ** from the list.
6. To add an IBM StoredIQ instance, select **Stored IQ** from the Adapter Configuration list.
7. In the Integration Instances section, click the **Add Instance** icon ⊕.
8. Set the following options.

Option	Description
Name	Specify IBM StoredIQ instance name.
URL	Specify the URL to access IBM StoredIQ. for example, `https://www.example.com/login`.
Microservice Instance	Select integration agent from the list.

Option	Description
User Name	Specify the IBM StoredIQ user name.
Password	Specify password for the user name.
Classifier and Vulnerability Assessment	Specify the configuration file to import data from integration server to IBM Data Risk Manager for risk analysis and actions.

9. Click **Save** to save the configuration details.

What to do next

For the adapter instance that you created, you can test the connectivity. Select the instance from the **Integration Instances** list, and then click **Test Connection** to test whether the communication between IBM StoredIQ instance and IBM Data Risk Manager server is successful.

Importing IBM StoredIQ data sources

You can import unstructured data sources from IBM StoredIQ into IBM Data Risk Manager inventory for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM StoredIQ. For more information about integration, see "Integrating IBM StoredIQ with IBM Data Risk Manager" on page 86.

About this task

The transaction icon indicates that the previous import operation was successful.

The transaction icon indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Source**.
4. Import data sources.

   a) Click the **Download** icon .

   b) On the **Import** window, select an IBM StoredIQ instance.

   c) Click **Import**.

      When the import operation is complete, the IBM StoredIQ data sources are added to the inventory.

   d) To refresh data source inventory list, click the **Refresh** icon .

   The data source that you added is listed on the **Data Source** page. Alternatively, you can also view the data sources that you imported on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **File Storage**.

Importing classifier scans from IBM StoredIQ

You can import classifier scans from IBM StoredIQ into IBM Data Risk Manager for risk analysis.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM StoredIQ. For more information about the integration, see "Integrating IBM StoredIQ with IBM Data Risk Manager" on page 86.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Scans**.
4. Import data scans.

   a) Click the **Download** icon .

   b) On the **Import Data Scans** window, from the **Adapter** list, select **StoredIQ**.

   c) From the **Instances** list, select an adapter instance. You can select up to three instances.

   d) Select **Classifier**.

   e) To import all the processes that are associated with the selected instances, click **Import**.

   f) To import only the IBM StoredIQ processes that you need from the selected instances, run the following steps.

      1) Click **Import with Process Selection**.

      2) Select the processes that you need to import from each adapter instance.

      3) Click **Import**.
5. On the **Data Scans** page, you can view the scans that you now imported.
6. To refresh data scan inventory list, click the **Refresh** icon .
7. Alternatively, to view scan results after the import operation, go to **Security Command and Control Center** > **Home**.

Administering users

User administration covers the tasks of adding and maintaining IBM Data Risk Manager users and groups, and associating users with roles to perform specific tasks within the applications.

IBM Data Risk Manager pre-defined user roles

A role is an object that defines the levels of authorization that is needed to perform product functions. To allow users to access the product functions, they must be mapped to the user roles. This mapping allows those users to access IBM Data Risk Manager components that are defined by the role.

The following user roles are defined in IBM Data Risk Manager:

- Administrator roles
- General roles

Administrator roles

The administrator role provides control over all the functions of IBM Data Risk Manager Application Suite. The different administrator roles are described in the following sections.

Super Administrator

The Super Administrator role provides control over all the functions and sub functions of IBM Data Risk Manager Application Suite. In addition, the Super Administrator is responsible for the following server administration functions.

- License management
- Integration adapter configuration
- Server configuration

BCM Administrator

The BCM Administrator role provides control over all functions in the Business Context Modeler (BCM) component of IBM Data Risk Manager Application Suite. The BCM Administrator acts as the security administrator of IBM Data Risk Manager and responsible for the user registration, user management, and role assignment activities. In addition, the BCM Administrator is responsible for the following tasks.

- Enterprise integration
- Program management
- Policy management
- Vulnerability assessment scans

C3 Administrator

The C3 Administrator role provides control over all functions in the Security Command and Control Center component of IBM Data Risk Manager Application Suite. The C3 Administrator is responsible for the following activities.

- Scheduling and triggering discovery scans
- Viewing, exporting, and managing remediation of vulnerability assessments

IDRM Administrator

The IDRM Administrator role provides control over all functions in the Security Command and Control Center component of IBM Data Risk Manager Application Suite. In addition to general dashboard functions, the IDRM Administrator is responsible for sending email notifications about database activity monitoring (DAM) alerts.

General roles

The general roles provide access to basic user functions of IBM Data Risk Manager Application Suite components.

BCM General

The BCM General role provides access to the following general-purpose functions of the BCM component.

- Native data source discovery
- Data flow modeling and business context modeling
- Remediation management

C3 General

The C3 General role provides access to the following general-purpose functions of the Security Command and Control Center component.

- Inventory management
- Iterative cleansing and analysis
- Taxonomy definition
- Action center

IDRM General

The IDRM General role provides access to general-purpose functions of IBM Data Risk Manager Dashboard.

Managing users

With the IBM Data Risk Manager user management function, administrators can create users, assign user roles, update user information, and change a user password.

IBM Data Risk Manager Server stores information about the users who can access various IBM Data Risk Manager components. Both authentication and authorization processes use the user information. The

Business Context Modeler (BCM) component provides Enterprise Integration Wizard (EIW) to create and manage users.

BCM Administrator role is needed to perform user management functions.

Creating a user account

You can create users and provide them access to IBM Data Risk Manager. Use the Enterprise Integration Wizard of Business Context Modeler to create users and manage their permissions.

Before you begin

You must have the BCM Administrator role to perform the user management functions.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application navigation icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **User**.
4. To create a user, click the **Add User** icon ⊕.
5. Set the following options and click **Save**.

Option	Description
User Type	You can specify any of the following types to log on to IBM Data Risk Manager. • **IDRM User** • **Single Sign-On** • **LDAP**
User Name	Specify the name of the user.
Password	Specify password for the user name.
Re-enter Password	Confirm the password.
Resource Name	Specify the resource name for the user you are creating. For the information about creating the resource name, see "Creating a resource to associate with the user" on page 91.
Email	Specify the email address of the resource. For the information about specifying the resource name, see "Creating a resource to associate with the user" on page 91.
Roles	Assign a role to the user you are creating.
Assign Program(s)	Assign programs to the user. Run the following steps to assign programs. For more information about programs, see "Managing programs" on page 124. a. Click **Assign Program(s)**. b. Select the programs that you want to assign. **Note:** You cannot assign a program for the user with **Super Administrator** role.

Creating a resource to associate with the user

You must add a resource and associate it to an IBM Data Risk Manager user credential that you are creating. To add a resource, you must specify the resource name and the email ID for the resource name.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application navigation icon ⠿.
3. Go to **Business Context Modeler** > **EIW** > **User**.
4. To create a user, click the **Add User** icon ⊕.
5. Specify the name of the user.
6. Specify the password details.
7. To create a resource name and the email for the user you are creating, click the **Resource Name** icon 👤.
    a) On the Resources page, click the add resource icon +.
    b) Specify the resource name that you want to associate with the user that you are creating.
    c) Specify the email ID of resource name.
    d) Click **Submit**.
       The resource name and the email ID are displayed in the **Resource Name** and **Email** fields.

   You can also associate an existing resource name to the user. Also, modify the resource name details.
8. Click **Save**.

Modifying user information

You can modify existing users, including their status as needed. You can also activate the disabled users within IBM Data Risk Manager.

Before you begin

You must have the BCM Administrator role to perform the user management functions.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application navigation icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **User**.
4. From the **Application Users** list, select the user name.
5. Modify the user information as needed
6. Click **Save**.

Changing a user password

Use the Enterprise Integration Wizard (EIW) that Business Context Modeler provides for changing the user password. The changed password of a user must comply with the password policy that IBM Data Risk Manager provides.

About this task

You must have the BCM Administrator role to perform the user management functions.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.

2. Click the application navigation icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **User**.
4. From the **Application Users** list, select the user name.
5. Select **Change Password**.
6. Specify the password information in the **Password** and **Re-enter Password** fields.
7. Click **Save**.

Disabling a user account

You can disable a user account to prevent the user from accessing IBM Data Risk Manager.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application navigation icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **User**.
4. From the **Application Users** list, select the user account for disabling.
5. Disable the **Enable User** toggle button.
6. Click **Save**.

Unlocking a user account

Administrator can unlock a user account that is locked when the number of allowable login retries is exceeded. Beyond the set number of allowable attempts with the wrong password, the account is locked.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application navigation icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **User**.
4. From the **Application Users** list, select the user account for unlocking.
5. Disable the **Account Locked** toggle button.
6. Click **Save**.

Managing user groups

A user group is a group of users. For more efficiency, consider creating a group that contains users who perform a similar task. You can create user groups, and assign individuals to the user groups in IBM Data Risk Manager.

IBM Data Risk Manager Business Context Modeler component provides Enterprise Integration Wizard (EIW) to create user groups. To create the user groups, following methods are used.

- Creating a user group by adding IBM Data Risk Manager users.
- Importing users that are created on the Lightweight Directory Access Protocol (LDAP) server into IBM Data Risk Manager. Importing into IBM Data Risk Manager is useful to maintain large user groups.

Creating a user group

Users can be combined into user groups to simplify administration in IBM Data Risk Manager.

Before you begin

You must have the BCM Administrator role to perform the user management functions.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.

2. Click the application navigation icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **User Group**.
4. To create a user group, click the **Add User Group** icon ⊕.
5. Set the following options and click **Save**.

Option	Description
Group Name	Specify the name of the user group.
Add Members	a. To add a member to the user group, click the **Add Members** icon ⊕. b. Select members from the list.
Group Members	Selected members of the group are displayed.

LDAP integration with IBM Data Risk Manager

SSO-LDAP integration aims at centralized Identity Management and single sign-on where users can sign on with their AD/LDAP credentials. You can import the user groups into IBM Data Risk Manager and assign specific roles to user for performing appropriate tasks in IBM Data Risk Manager.

IBM Data Risk Manager uses the following micro service to enable single sign-on and to import user groups from Active Directory (AD) servers.

```
Identity Manager (Consuming the User groups) – runs on port 8765
```

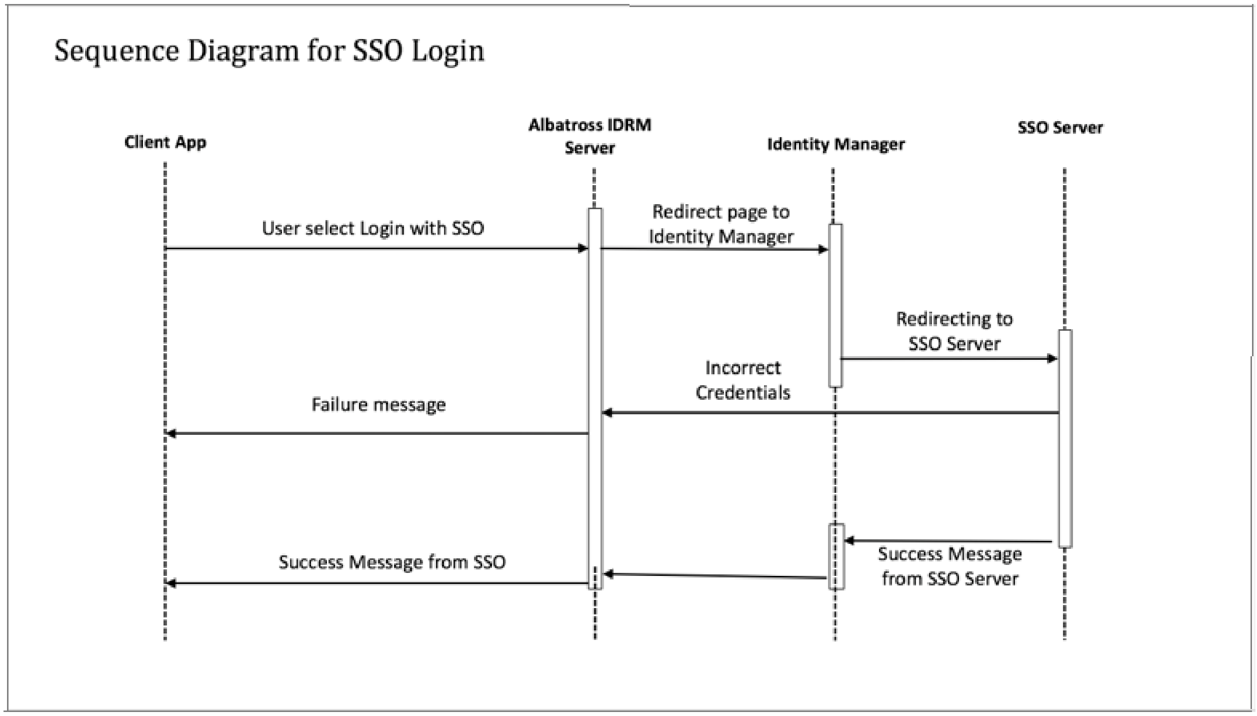
For more information on prerequisites, see “Installation prerequisites” on page 17.

Ensure that the IBM Data Risk Manager Server image or build is available in the necessary format based on the environment where you are running the installation.

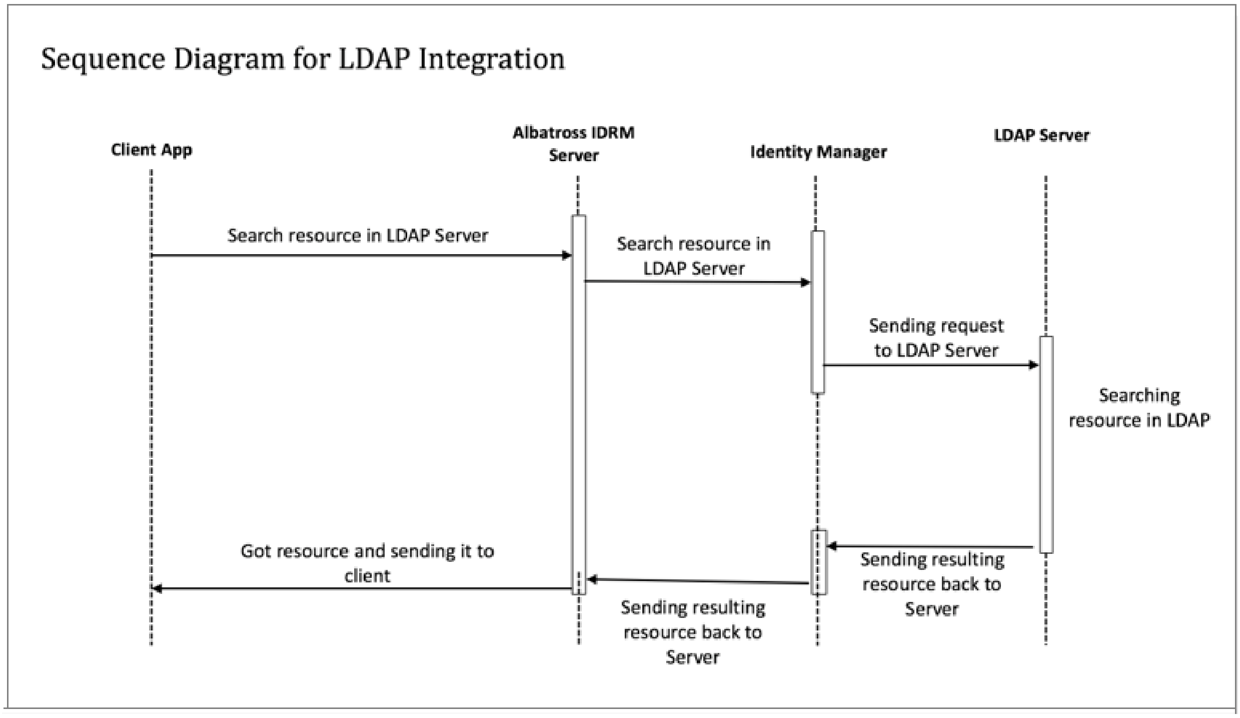
You can configure IBM Data Risk Manager to establish connection with an LDAP directory or an SSO service.

- The LDAP directory or SSO service must be running on a host that is accessible to IBM Data Risk Manager Server.
- For LDAP integration, an LDAP account must be available with known user names and passwords for IBM Data Risk Manager to use.
- Ensure that the Fully Qualified Domain Name (FQDN) of the LDAP server is available.
- Ensure that the port on which IBM Data Risk Manager communicates with the LDAP server is free. The default port number is 389.
- For SSO, you must provide either the IDP XML file or the URL of the SSO service.
- For any self-signed certificate that is associated with the IDP file, you must provide the certificate key and password.

Workflow of SSO integration into IBM Data Risk Manager


Sequence Diagram for SSO Login
Client App
Albatross IDRM Server
Identity Manager
SSO Server
User select Login with SSO
Redirect page to Identity Manager
Redirecting to SSO Server
Incorrect Credentials
Failure message
Success Message from SSO Server
Success Message from SSO

Workflow of LDAP integration into IBM Data Risk Manager


Sequence Diagram for LDAP Integration
Client App
Albatross IDRM Server
Identity Manager
LDAP Server
Search resource in LDAP Server
Search resource in LDAP Server
Sending request to LDAP Server
Searching resource in LDAP
Sending resulting resource back to Server
Got resource and sending it to client
Sending resulting resource back to Server

Integrating LDAP with IBM Data Risk Manager

Integrate IBM Data Risk Manager with Lightweight Directory Access Protocol (LDAP) server to import user groups that are created in LDAP server. Importing user groups into IBM Data Risk Manager is useful to maintain large user groups.

Before you begin

For prerequisite information, see "LDAP integration with IBM Data Risk Manager" on page 93.

About this task

Procedure

1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⋮⋮⋮.
3. Click **Administration**.
4. Click **Server Configuration** > **SSO and LDAP Configuration**.
5. Select the micro service from the list.
6. Configure Single Sign-On (SSO).
   a) Select **Enable SSO**.
   b) Specify the SSO login URL in **SSO Login URL**.
   c) Select the IDP configuration type, such as `File` or `URL`.
      - If you select `File`, click **Choose File** to locate and upload the IDP configuration file.
      - If you select `URL`, specify the URL in **Enter IDP XML URL**.
   d) Click **Save Configuration**.
7. Configure LDAP.
   a) Select **Enable LDAP**.
   b) Select the authentication type `Simple` from **LDAP Authentication Type**.
   c) Specify the LDAP provider URL in **Provider URL**. For example, `ldaps://example.com:636`.
   d) Specify domain component for the user groups in **Domain Component for User Groups**. For example, `ou=bluepages,o=ibm.com`.
   e) Specify the domain component for users in **Domain Component for Users**. For example, `ou=bluepages,o=ibm.com`.
   f) Specify name of the attribute that stores the user name on the LDAP server in **LDAP Login User Name Attribute**. For example, `uid`.
   g) Specify the pattern for login user name in **LDAP Login User Name Pattern**. For example, `uid={0},ou=bluepages,ou=in,ou=ibm`
   h) Specify the IBM Data Risk Manager login user name attribute in **IBM Data Risk Manager User Name Attribute**. For example, `email`.
   i) Specify the database user name attribute in **Database User Name Attribute**.
   j) To specify user name and password for the LDAP administrator account, select **Admin Credentials**.
      1) Specify the user name in **LDAP User Name**.
      2) Specify password for the user name in **LDAP Password**.
   k) To Specify the group login information, select **Group Login**.
      1) Specify the attribute that contains the name of the group, as defined in the LDAP directory in **Group Name Attribute**. For example, `cn={gName}`.
      2) Specify the group user name attribute in **Group User Name Attribute**. For example, `uid`.

    3) Specify the attribute that contains a user in a group, as defined in the LDAP directory in **Group Member Attribute**. For example, `uniqueMember`.
    4) Specify the group list base DN in **Group List Base DN**. For example, `ou=memberlist,ou=ibmgroups`.

  l) Select **User Base DN Fields** to configure the Base Distinguished name (Base DN) with which to begin your LDAP search.

  A dynamic group defines its members by using an LDAP search. If you select **Dynamic User Base DN**, you must specify the value in **User Base DN Pattern**. For example, `uid={0},c={1},ou={2}`.

  A static group defines its members by listing them individually. If you select **Static User Base DN**, you must specify the value in **User Base DN** .

  m) Click **Save Configuration**.

Sample LDAP configuration file.

```
com.agile3.config.ldapProviderUrl=ldaps://example.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
```

Importing a user group

You can import users that are created on the Lightweight Directory Access Protocol (LDAP) server into IBM Data Risk Manager. Importing into IBM Data Risk Manager is useful to maintain large user groups.

Before you begin

You must have the BCM Administrator role to perform the user management functions.

You must configure the LDAP server information by using the IBM Data Risk Manager Administration component. For LDAP configuration information, see "Integrating LDAP with IBM Data Risk Manager" on page 95.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the application navigation icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **User Group**.
4. To import a user group, click the **Import Group** icon ⤓.
5. Select the agent from the list for connecting to the LDAP server.
6. Select the user group from the list to import.
7. Click **Save**.

Discovering native data sources

By using the Network Mapper (NMAP) utility, you can run a port scan on an IP range to discover native data sources or hosts in a network segment. You can also define data sources by importing files in a comma-separated value (CSV) format that contain data source inventory.

Use IBM Data Risk Manager Enterprise Integration Wizard (EIW) to discover native data sources.

Running port scan to discover data sources

Run the port scan by using Network Mapper (NMAP) on the specified IP address range to discover data sources or hosts in the target network.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Native Discovery**.
4. Set the following options on the **Native Data Source Scanning with Nmap** page.

Option	Description
Single IP	Specify an IP address to scan a single port.
Range of IPs	Specify the IP address range for scanning.
Port Number	Specify a port number or port range for scanning.

5. Click **Scan** to trigger a port scan in the target IP and port range.
6. Click **History** to view and track scan status on the **Scans** window.
7. When the scan is complete, select a completed scan item on the **Scans** window. Potential data sources in the scanned port range are listed on the **IP Scans** page.

What to do next

You can add a data source to the discovered data source repository. For more information about adding a data source, see "Adding a data source" on page 97.

Adding a data source

You can add a data source to the IBM Data Risk Manager inventory for the data sources that are discovered when the port scan was run.

Procedure

1. Run the port scan.

   For the steps on how to run a port scan, see "Running port scan to discover data sources" on page 97.
2. When the scan is complete, select the completed scan item on the **Scans** page. Associated data sources in the scanned port range are listed on the **IP Scans** page.
3. On the **IP Scans** page, click the scanned IP address. Associated data sources in the scanned port range are listed.
4. To add a data source, click the **Add Data Source** icon +.
5. Set the following options and click **Add**.

Option	Description
Adapter	Data collector name.
Agents	Agent name to connect to the database.
Database Name	Name of the database.
Identifier	Name for the data source.
User Name	Name of the database user.
Password	Password for the database user name.

6. To view the data sources that you added, click **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.

Importing data sources into IBM Data Risk Manager from a CSV file

You can add data sources to IBM Data Risk Manager inventory for discovery, classification, and other purposes by importing a comma-separated value (CSV) file that contains data source information.

About this task

A CSV file is a data file consisting of fields and records that are stored as text. In which, the fields are separated from each other by commas. If the data in a field contains a comma, the field is surrounded with quotation marks. The first line of the file can contain the descriptive names of the variables (columns). You might include these column titles, `Data Source Name`, `IP Address`, `Port Number`, `DB Type`,`Database Name`, `Delete` as shown in the following example.

Data Source Name	IP Address	Port	DB Type	Database Name	Delete
Oracle on 45 DS	X.XXX.XXX.XX	1521	Oracle	ORCL	FALSE
MySQL on Aceva D	X.XXX.XXX.XX	3306	MYSQL	Northwind	FALSE

Where,

Data Source Name
An identifier to uniquely distinguish the database.

IP Address
IP Address of the database server or instance.

Port
Port number for connecting to the database.

DB Type
Database type, such as Oracle, MSSQL, Db2, Sybase, PostgreSQL, or MySQL.

Database Name
Name of the database.

Delete
Defaulted to FALSE for the creation of data source. If the value is set to TRUE, data source is deleted from the IBM Data Risk Manager Server after the import operation.

With the necessary information for each target database, IBM Data Risk Manager data source definition import template can be used to define data sources.

Procedure

1. Define data source information in the CSV template file.
2. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).

3. Click the application menu icon ⠿.
4. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Native Discovery**.
5. Click **Import**.
6. To locate and select the data source definitions CSV file, click **Choose File**.
7. Click **Load**. Data sources are displayed in the **Import Data Source** section.

   If an error is encountered, then you need to review your CSV file to correct errors, and import the file again. If the data source list is structured incorrectly or the data source list contains incorrect information, import of the CSV file might fail.
8. Specify connection parameters to the data sources that are imported to establish connection to the database.

   a. Select a database and double-click.

   b. Set the following options and click **Add**.

Adapter	Data collector name.
Agents	Agent name to connect to the database.
Database Name	Name of the database.
Identifier	Name for the data source.
User Name	Name of the database user.
Password	Password for the database user name.

9. To view the data sources that you added, click **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.

Mapping business context data

IBM Data Risk Manager provides visibility to information asset risks in the business context data of an organization. To get this visibility, an understanding of business processes, applications, data assets, access to critical information, and other business entities and their usage are needed.

Typically, business context data of an organization is stored in a Configuration Management Database (CMDB), for example ServiceNow. Alternatively, the data can also be acquired through questionnaires, interviews, and workshops with key client stakeholders.

Importing business context data by using CSV files

Viewing information asset risks requires an initial one-time capture and import of organizational business context data in terms of business units, lines of business (LOB), business processes, applications, and stakeholders. You can import the business context data into IBM Data Risk Manager by using one or multiple files in comma-separated values (CSV) format. The organization metadata is mapped to the IBM Data Risk Manager meta model, and then the dashboard views can be configured for the risk analysis.

When the business context mapping is complete, organization context data can be imported into the system based on completed mappings. If the mapping is updated, organization context data must be imported again to maintain data integrity.

Business context mapping consists of the following steps.

1. Preparing business context data for import.
2. Loading business context data for mapping.
3. Mapping business context data.
4. Configuring the IBM Data Risk Manager views.

5. Storing the content and structural format on the IBM Data Risk Manager server.

If you want to import the context data again where only data in the CSV files is updated without any additional columns, run the following steps.

1. Preparing business context data for import.
2. Loading business context data for mapping.
3. Storing the content and structural format on the IBM Data Risk Manager server.

Viewing and managing business context data

You can use the **Manage Inventory** component to easily and quickly view and manage applications and business processes that you imported through CSV files as context data and their associations with other business entities. For more information about managing the context data, see "Application inventory" on page 116 and "Business process inventory" on page 119.

Importing ServiceNow CMDB into IBM Data Risk Manager

You can configure ServiceNow to import configuration management database (CMDB) data into IBM Data Risk Manager and use this data along with applications and business context.

For more information about how to import ServiceNow CMDB into IBM Data Risk Manager, see "Integrating ServiceNow with IBM Data Risk Manager" on page 69.

Preparing business context data for import

To map business context data, you must capture or prepare the context data for importing into IBM Data Risk Manager.

About this task

In an organization, the business context information can be found in a Configuration Management Database (CMDB) type of systems or in worksheets that are maintained by the database management teams. Organizations might have an application inventory that is maintained manually or in enterprise architecture applications that contain information about associated business processes, departments, stakeholders, or other relevant metadata. If the business context information is not available, data can be captured through surveys and information gathering sessions that are conducted with stakeholders in the organization.

The following categories of organization context data sets can be imported into IBM Data Risk Manager.

- Database
- Application
- Business Process

The data sets that are associated with the three categories can be captured in a single or multiple CSV files. A common field (link field) must exist for tying the three data sets together. For example, an application identifier can be the link field. Application is the entity in most of the organizations that tie the business processes and other business metadata to the data repositories where the data is stored.

Procedure

Prepare the contents of the CSV files for Database, Application, and Business Process categories that are relevant to the organization.

What to do next

Load the business context metadata. For more information about how to load the data sets, see "Loading business context data" on page 101.

Loading business context data

You must load the business context data for mapping to IBM Data Risk Manager metadata glossary.

Before you begin

Ensure that the business context data is available for loading. For more information about preparing the context data, see "Preparing business context data for import" on page 100.

You can download the sample templates at: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Number of columns in the context data CSV files that you import to IBM Data Risk Manager must not exceed 49.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization** > **Load Business Context**.
4. To select data files, select **Load Configuration and Data Files**.

   a) Click the CSV file icon CSV to select `Database`, `Application`, and `Business Process` CSV files.

   Select **Load Data Files** to load files where data is updated without any additional columns to the CSV files that are already imported.
5. Click **Next**.

What to do next

Map the business context data to IBM Data Risk Manager metadata glossary for specifying the business taxonomy of discovered information assets. For more information about how to map the context data, see "Mapping business context data" on page 101.

Mapping business context data

You must map the business context data to IBM Data Risk Manager metadata glossary for specifying the business taxonomy of discovered information assets.

Before you begin

Ensure that the business context data is loaded into IBM Data Risk Manager. For more information about how to load business context data, see "Loading business context data" on page 101.

About this task

Mapping of context data is a one-time activity, and a prerequisite step for importing data. Mapping of attributes to business glossary of IBM Data Risk Manager can be updated at any time. However, any changes to the mapping must be followed by import of the context data to ensure complete mapping.

One attribute from `Database`, `Application`, and `Business Process` metadata must be selected as a common field or `Link Field` to map attributes across the three different entities.

By default, all business context entity attributes are marked as `Property`, which is a general-purpose attribute. Apart from this attribute, Business Context Modeler identifies the following four categories of attributes.

DB Resolution

Represents data that is specific to the organization data infrastructure. The data includes attributes that help identify databases information for ingestion into IBM Data Risk Manager. The following attributes are necessary for DB resolution and are listed as subproperty type.

- Database Name
- IP Address
- Server
- Name
- DB Type

Entitlements

Represents metadata that can be used for defining scope for data discovery and classification. For example, `Environment` is an entitlement property that can be used to scope the data discovery to run in production, test or development databases. Following entitlement attributes are defined in the IBM Data Risk Manager meta model.

- Compliance
- Environment
- Line of Business

Taxonomy Mapping

Represents data that is specific to the business context visualization in IBM Data Risk Manager. These attributes are used during the taxonomy definition and assignment. Following taxonomy mapping attributes are defined in the IBM Data Risk Manager meta model.

- Group **–** Organization Level
- Application
- Business Support Process
- Consumer Organization Level 2
- Consumer Organization Level 1

Resource

Identifies the attribute to be a role or a resource.

Note: If the configuration information of the previous context data import is available in the system, mapping information is restored for the similar attributes.

Procedure

1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization** > **Map Business Context**.
2. To map attributes across the three different entities, select a common field or link field from the **Link Field** drop-down list. For example, `APP_ASSETID`.
3. Click **DB Resolution** to map the DB resolution attributes.

   a) Click the add icon ⊕ next to the attribute, and specify the CSV file column name in **Search Columns**.

   For example, to map DB_Name to `Database Name` in the CSV file, specify `Database Name` in **Search Columns**. The column name is displayed and mapped.

   b) Map the remaining attributes to the corresponding columns of the CSV file.
4. Click **Entitlements** to map the entitlements attributes.

   a) Click the add icon ⊕ next to the attribute, and specify the CSV file column name in **Search Columns**.

   For example, to map `Compliance` to SOX in the CSV file, specify SOX in **Search Columns**. The column name is displayed and mapped.

   b) Map the remaining attributes to the corresponding columns of the CSV file.

5. Click **Taxonomy Mapping** to map the taxonomy attributes.

   a) Click the add icon ⊕ next to the attribute, and specify the CSV file column name in **Search Columns**.

   For example, to map `Consumer Organization Level 1` to `Business_Support_Consuming_Organization_Level_1` in the CSV file, specify `Business_Support_Consuming_Organization_Level_1` in **Search Columns**. The column name is displayed and mapped.

   b) Map the remaining attributes to the corresponding columns of the CSV file.

6. Click **Resource** to map the entitlements attributes.

   a) Click the add icon ⊕ next to the attribute, and specify the CSV file column name in **Search Columns**.

   For example, to map `Product Owner` to `Application_Owner` in the CSV file, specify `Application_Owner` in **Search Columns**. The column name is displayed and mapped.

   b) Map the remaining attributes to the corresponding columns of the CSV file.

7. Click **Next**.

What to do next

Configure IBM Data Risk Manager Dashboard. For more information about how to configure the dashboard, see "Configuring IBM Data Risk Manager Dashboard" on page 103.

Configuring IBM Data Risk Manager Dashboard

You must configure IBM Data Risk Manager dashboard widgets to display the attributes that are mapped.

Before you begin

Ensure that the business context data is mapped to IBM Data Risk Manager metadata glossary. For more information about how to map the context data, see "Mapping business context data" on page 101.

About this task

You can configure the attributes in the following IBM Data Risk Manager Dashboard widgets by using the drag-and-drop mechanism.

- Infrastructure
- Application
- Business Process
- Resource

Note: If the configuration information of the previous context data import is available in the system, dashboard configuration information is restored. If necessary, you can modify the configuration.

Procedure

1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization** > **Configure IBM Data Risk Manager Dashboard**.
2. Click the attribute icon under **Assigned Properties**, and then drag on corresponding attribute name in the IBM Data Risk Manager dashboard widget. The mapped attribute name is then displayed under **Data Risk Manager Attribute**.

For example, click the **ENV** icon under **Database** > **Assigned Properties**, and then drag on **Environment** in the **IDRM Mapping** > **Infrastructure** widget. The dropped attribute name is then displayed under **Data Risk Manager Attribute**.

3. Configure IBM Data Risk Manager dashboard widgets with the remaining attributes from **Database**, **Application**, and **Business Process**.
4. To configure the **Resource** widget, the attributes that are to be dragged must be of property type `Resource`. Stakeholder responsibility assignment follows the RACI matrix for key roles that are defined in the context data. Drag the **Resource** icon on pie slices under the **Resource** widget.
5. Click **Next**.

What to do next

You can create groups and assign attributes to them based on a business context. For more information see, “Mapping IBM Data Risk Manager properties” on page 104.

When you click **Next**, you are prompted to save the settings for attributes mapping and dashboard configuration. To proceed, click **Yes**. For more information about how to save settings and import the context data, see “Importing business context data” on page 105.

Mapping IBM Data Risk Manager properties

You can configure IBM Data Risk Manager dashboard widgets to display the attributes, which are configured and grouped based on a business context, in a pop-over window.

Procedure

1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization** > **Configure IBM Data Risk Manager Dashboard** > **IDRM Property Mapping**.
2. Create groups for attributes from **Database**, **Application**, and **Business Process** categories and add attributes to the group.

   Run the following steps to create a group.

   a. Select **Database**, **Application**, or **Business Process** according to your requirements.
   b. Click **Add Group**.
   c. Specify a group name.
   d. To assign group name to all the unassigned columns, select **Assign the group to unassigned columns**.
   e. Click **Save**.

   Run the following steps to add attributes to a group.

   a. Select a group.
   b. Select an attribute from the list.
   c. Specify the attribute name to be displayed on the dashboard widget pop-over.
   d. To select the data field type to be displayed for attribute on the widget pop-over, click the drop-down icon. For example, Text field, checkbox, flag, or pie chart.
   e. Repeat the same steps for all the attributes according to the requirements.
3. To clear property mapping information, click the clear mapping icon
4. Click **Next**.

What to do next

When you click **Next**, you are prompted to save the settings for attributes mapping and dashboard configuration. To proceed, click **Yes**. For more information about how to save settings and import the context data, see "Importing business context data" on page 105.

Importing business context data

Import the context data to map context data to the business glossary of IBM Data Risk Manager for specifying the attributes that are related to databases, applications, and business processes.

Before you begin

Ensure that all the attributes are configured in the various dashboard widgets. For more information about how to configure IBM Data Risk Manager dashboard widgets, see "Configuring IBM Data Risk Manager Dashboard" on page 103.

About this task

After you save the settings for attributes mapping and dashboard configuration, you are prompted to import the business context data. Click **Yes** to proceed.

Procedure

1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization** > **Validate Business Context Import**.
2. When prompted, click **Yes** to proceed with saving the configuration settings and data import.
3. The contents are displayed in a tabular format. Click **Save** to save the settings.
4. When prompted, click **Yes** to import the context data. The organization-specific data files and configuration settings are imported into IBM Data Risk Manager.

   Note: If the mapping information is incorrect, a mapping summary sheet is displayed to view the data. You must correct the mapping information to proceed with the import operation.

Managing inventory

Use the Manage Inventory component to view and manage IBM Data Risk Manager inventory items such as data sources, applications, business processes, information assets, and threats.

Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** to view and manage the following inventory items.

Application
View and manage all applications in IBM Data Risk Manager inventory. For more information about how to manage application inventory, see "Application inventory" on page 116.

Business Process
View and manage all business processes in IBM Data Risk Manager inventory. For more information about how to manage business process inventory, see "Business process inventory" on page 119.

Data Source
View and manage all data sources in IBM Data Risk Manager inventory. For more information about how to manage data source inventory, see "Data source inventory" on page 106.

Threat
View and manage all possible threats IBM Data Risk Manager inventory. For more information about how to manage data source inventory, see "Threat inventory" on page 122.

Data source inventory

You can view and manage all data sources that IBM Data Risk Manager inventory contains from a single location to track your data source information.

Data source can be a repository where the data of an organization is stored. IBM Data Risk Manager supports both structured data, such as databases, and unstructured data, such as file shares. You can define and manage various data sources in IBM Data Risk Manager.

Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** to view and manage the data sources.

Viewing data source inventory

You can easily view and manage data source information from a single location. Use the **Manage Inventory** > **Data Source** component to track all the sources from which the data is added or imported to IBM Data Risk Manager inventory for data discovery and classification operations.

About this task

You must relate business context information that includes enterprise applications, business processes, and stakeholders with sensitive data discovered from various sources. For more information about business context data, see "Mapping business context data" on page 99.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. To view list of data sources from various sources and their attributes, go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.
4. On the **Create/Update Inventory** page, select a data source type such as **Database**, **File Storage**, **Application**, or **Server** to view associated data sources and their attributes in tabular format.
5. To add a data source to the inventory, select a source type and click the **Add Data Source** icon ⊕.
6. For a selected data source, click the **Actions** icon ••• to run the following operations based on the selected data source type.
   - To modify data source information, click the **Edit** icon ✎.

     Note: You cannot edit details of the data sources of type **Application**.
   - To delete a data source from the inventory, click the **Delete** icon 🗑.

     Note: You can delete only the IBM Data Risk Manager native data sources and IBM Security Guardium data sources from the inventory.
   - You can limit display of data sources in the list based on the filter option that you select. Click the filter icon ⏷ to select your filter option.
7. For a selected data source, you can also view the following information.

Icon	Description
♔	Indicates that the data contains crown jewel information.
🖧	Indicates that the data is classified.
01🔒	Indicates that the data contains sensitive information.

Icon	Description
🇺🇸	Country flag indicates where the data source resides.
✓	Indicates that the data source is mapped with business context entities.

Adding data sources to inventory

You can add data sources to IBM Data Risk Manager inventory from multiple sources to evaluate risks that are associated with the data assets.

Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** to add the data sources.

Adding a native data source

You can add a native structured data source into IBM Data Risk Manager inventory to make its data available for risk analysis and actions.

Before you begin

Before you create a data source, you must be aware of the database connection parameters for the data source you want to connect to.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.
4. To add a native structured data source, click the **Add Data Source** icon ⊕.
5. On the **Add Data Source** page, specify the database properties for the data source and click **Add**.

Option	Description
Server Type	Database server that you want to use. For example, **Oracle**. For MSSQL server, if the server is enabled to use Windows authentication, you can connect to the database by using Windows user login credentials for authentication. Run the following steps for Windows-based authentication for MSSQL server. a. Select **Enable Domain Authentication**. b. Specify domain name of the server in the **Domain Name** field.
Data Source Name	A unique name for the data source.
IP Address	IP address of the database server.
Port	Listening port number of the database server.
Database Name	Name of the database.
Adapter	Adapter instance name. For example, `Native Structured`.
Agents	Agent name to connect to the data source.
User Name	Name of the user for connecting to the data source.

Option	Description
Password	Password for the database user name.
Encryption	Encryption status of the data source server.
Monitoring	Status of database monitoring agent.
Custom URL	Custom URL connection string to the data source.
Geographic Location	Geographic location of the data source.

The data source that you added is listed on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **Database**.

Adding native unstructured data source

You can add native unstructured data sources into IBM Data Risk Manager inventory for risk analysis and actions.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.
4. To add an unstructured data source, click the **Add Data Source** icon ⊕.
5. On the **Add Data Source** page, set the following options and click **Add**.

Option	Description
Server Type	Data source server type that you want to use. For example, **IDRM**.
Target	Name for the data source.
IP Address	IP address of the data source server.
Port	Port number for connecting to the data source server.
Port Type	File sharing protocol to access data.
Target Path	Target path to import unstructured data.
Adapter	Adapter instance name. For example, `Native Unstructured`.
Agents	Agent name to connect to the data source.
User Name	Name of the user.
Password	Password for the user name.
Encryption	Encryption status of the data source server.
Monitoring	Status of monitoring agent.
Geographic Location	Geographic location of the data source.

The data source that you added is listed on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **File Storage**.

Adding IBM Security Guardium data sources

You can add IBM Security Guardium data sources into IBM Data Risk Manager inventory to make the data available for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security Guardium. For more information about integration, see "Integrating IBM Security Guardium with IBM Data Risk Manager" on page 36.

Before you create a data source, you must be aware of the database connection parameters for the data source you want to connect to.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.
4. To add IBM Security Guardium data source, click the **Add Data Source** icon ⊕.
5. On the **Add Data Source** page, set the following options and click **Add**.

Option	Description
Server Type	Database server type that you want to use. For example, `MySQL`.
Data Source Name	A unique name for the data source.
IP Address	IP address of the database server.
Port	Listening port number of the data source.
Database Name	Name of the database.
Adapter	IBM Security Guardium instance name. For example, `Guardium_Adapter`.
Agents	Agent name to connect to the database.
User Name	Name of the user for connecting to the database.
Password	Password for the database user name.
Encryption	Encryption status of the data source server.
Monitoring	Status of database monitoring agent, such as S-TAP.
Custom URL	Custom URL connection string to the data source.
Geographic Location	Geographic location of the data source.

The data source that you added is listed on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **Database**.

Adding Symantec DLP data sources

You can add Symantec DLP data sources into IBM Data Risk Manager inventory for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with Symantec DLP. For more information about integration, see "Integrating Symantec DLP with IBM Data Risk Manager" on page 64.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.
4. To add a Symantec DLP data source, click the **Add Data Source** icon ⊕.
5. On the **Add Data Source** page, set the following options and click **Add**.

Option	Description
Server Type	Data source server type that you want to use. For example, **IDRM**.
Target	Name for the data source.
IP Address	IP address of the data source server.
Port	Port number for connecting to the server.
Port Type	File sharing protocol to access data.
Target Path	Target path to import unstructured data.
Adapter	Symantec DLP instance name. For example, `Symantec DLP Instance`.
Agents	Agent name to connect to the data source.
User Name	Name of the user.
Password	Password for the user name.
Encryption	Encryption status of the data source server.
Monitoring	Status of monitoring agent data source server.
Geographic Location	Geographic location of the data source.

The data source that you added is listed on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **File Storage**.

Adding IBM Security AppScan Enterprise data sources

You can add IBM Security AppScan Enterprise data sources into IBM Data Risk Manager inventory for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security AppScan Enterprise. For more information about integration, see "Integrating IBM Security AppScan Enterprise with IBM Data Risk Manager" on page 57.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.
4. To add IBM Security AppScan Enterprise data source, click the **Add Data Source** icon ⊕.

5. On the **Add Data Source** page, set the following options and click **Add**.

Option	Description
Server Type	Server type that you want to use. For example, **IBM Appscan**.
Data Source Name	A unique name for the data source.
Host URL	URL of the host server to import data.
IP Address	IP address of the server.
Port	Port number for connecting to the server.
Adapter	IBM Security AppScan Enterprise instance name. For example, `AppScan_Instance`.
Agents	Agent name to connect to the server.
User Name	Name of the user for connecting to the server.
Password	Password for the user name.
Encryption	Encryption status of the data source server.
Monitoring	Status of the monitoring agent.
Geographic Location	Geographic location of the data source.

The data source that you added is listed on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **Application**.

Adding IBM QRadar Security Intelligence Platform data sources

You can add IBM QRadar Security Intelligence Platform data sources into IBM Data Risk Manager inventory for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM QRadar Security Intelligence Platform. For more information about integration, see Integrating IBM QRadar Security Intelligence Platform with IBM Data Risk Manager.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.
4. To add IBM QRadar Security Intelligence Platform data source, click the **Add Data Source** icon ⊕.
5. On the **Add Data Source** page, set the following options and click **Add**.

Option	Description
Server Type	Data source server type that you want to use, for example `Server`.
Data Source Name	Name for the data source.
IP Address	IP address of the data source server.

Option	Description
Adapter	IBM QRadar Security Intelligence Platform instance name. For example, `Qradar_Adapter`.
Agents	Agent name to connect to the data source.
User Name	Name of the user.
Password	Password for the user name.
Encryption	Encryption status of the data source server.
Monitoring	Status of the monitoring agent.
Geographic Location	Geographic location of the data source.

The data source that you added is listed on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **Server**.

Importing data sources to inventory

You can import data sources to IBM Data Risk Manager inventory from multiple sources to evaluate risks that are associated with the data assets.

Importing IBM Security Guardium data sources

You can import data sources from IBM Security Guardium appliances into IBM Data Risk Manager inventory for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security Guardium. For more information about integration, see "Integrating IBM Security Guardium with IBM Data Risk Manager" on page 36.

About this task

The transaction icon indicates that the previous import operation was successful.

The transaction icon indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Source**.
4. Import data sources.

   a) Click the **Download** icon.

   b) On the **Import** window, select an IBM Security Guardium adapter instance.

   c) Click **Import**.

   When the import operation is complete, the IBM Security Guardium data sources are added to the inventory.

   d) To refresh data source inventory list, click the **Refresh** icon.

The data source that you added is listed on the **Data Source** page. Alternatively, you can also view the data sources that you imported on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **Database**.

Importing IBM Security AppScan Enterprise data sources

You can import data sources from IBM Security AppScan Enterprise into IBM Data Risk Manager inventory for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security AppScan Enterprise. For more information about integration steps, see "Integrating IBM Security AppScan Enterprise with IBM Data Risk Manager" on page 57.

About this task

The transaction icon indicates that the previous import operation was successful.

The transaction icon indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Source**.
4. Import data sources.

   a) Click the **Download** icon.

   b) On the **Import** window, select an IBM Security AppScan Enterprise instance from the list.

   c) Click **Import**.

   When the import operation is complete, the IBM Security AppScan Enterprise data sources are added to the inventory.

   d) To refresh data source inventory list, click the **Refresh** icon.

   The data source that you added is listed on the **Data Source** page. Alternatively, you can also view the data sources that you imported on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **Application**.

Importing IBM QRadar Security Intelligence Platform data sources

You can import data sources from IBM QRadar Security Intelligence Platform into IBM Data Risk Manager inventory for data classification and risk analysis.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM QRadar Security Intelligence Platform. For more information about integration steps, see "Integrating IBM QRadar Security Intelligence Platform with IBM Data Risk Manager" on page 50.

About this task

The transaction icon indicates that the previous import operation was successful.

The transaction icon indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Source**.
4. Import data sources.

   a) Click the **Download** icon.

   b) On the **Import** window, select an IBM QRadar Security Intelligence Platform instance from the list.

   c) Click **Import** tab.

   When the import operation is complete, the IBM QRadar Security Intelligence Platform data sources are added to the inventory.

   d) To refresh data source inventory list, click the **Refresh** icon.

   The data source that you added is listed on the **Data Source** page. Alternatively, you can also view the data sources that you imported on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **Server**.

Importing IBM Security Guardium Analyzer data sources

You can import data sources from IBM Security Guardium Analyzer into IBM Data Risk Manager inventory for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security Guardium Analyzer. For more information about integration, see "Integrating IBM Security Guardium Analyzer with IBM Data Risk Manager" on page 82.

About this task

The transaction icon ✓ indicates that the previous import operation was successful.

The transaction icon ! indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Source**.
4. Import data sources.

   a) Click the **Download** icon.

   b) On the **Import** window, select an IBM Security Guardium Analyzer instance.

   c) Click **Import**.

   When the import operation is complete, the IBM Security Guardium Analyzer data sources are added to the inventory.

   d) To refresh data source inventory list, click the **Refresh** icon.

The data source that you added is listed on the **Data Source** page. Alternatively, you can also view the data sources that you imported on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **Database**.

Importing IBM StoredIQ data sources

You can import unstructured data sources from IBM StoredIQ into IBM Data Risk Manager inventory for risk analysis and actions.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM StoredIQ. For more information about integration, see "Integrating IBM StoredIQ with IBM Data Risk Manager" on page 86.

About this task

The transaction icon indicates that the previous import operation was successful.

The transaction icon indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Source**.
4. Import data sources.

   a) Click the **Download** icon .

   b) On the **Import** window, select an IBM StoredIQ instance.

   c) Click **Import**.

   When the import operation is complete, the IBM StoredIQ data sources are added to the inventory.

   d) To refresh data source inventory list, click the **Refresh** icon .

   The data source that you added is listed on the **Data Source** page. Alternatively, you can also view the data sources that you imported on the **Create/Update Inventory** page under **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source** > **File Storage**.

Importing data sources into IBM Data Risk Manager from a CSV file

You can add data sources to IBM Data Risk Manager inventory for discovery, classification, and other purposes by importing a comma-separated value (CSV) file that contains data source information.

About this task

A CSV file is a data file consisting of fields and records that are stored as text. In which, the fields are separated from each other by commas. If the data in a field contains a comma, the field is surrounded with quotation marks. The first line of the file can contain the descriptive names of the variables (columns). You might include these column titles, `Data Source Name`, `IP Address`, `Port Number`, `DB Type`,`Database Name`, `Delete` as shown in the following example.

Data Source Name	IP Address	Port	DB Type	Database Name	Delete
Oracle on 45 DS	X.XXX.XXX.XX	1521	Oracle	ORCL	FALSE
MySQL on Aceva D	X.XXX.XXX.XX	3306	MYSQL	Northwind	FALSE

Where,

Data Source Name
An identifier to uniquely distinguish the database.

IP Address
IP Address of the database server or instance.

Port
Port number for connecting to the database.

DB Type
Database type, such as Oracle, MSSQL, Db2, Sybase, PostgreSQL, or MySQL.

Database Name
Name of the database.

Delete
Defaulted to FALSE for the creation of data source. If the value is set to TRUE, data source is deleted from the IBM Data Risk Manager Server after the import operation.

With the necessary information for each target database, IBM Data Risk Manager data source definition import template can be used to define data sources.

Procedure

1. Define data source information in the CSV template file.
2. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
3. Click the application menu icon ⠿.
4. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Native Discovery**.
5. Click **Import**.
6. To locate and select the data source definitions CSV file, click **Choose File**.
7. Click **Load**. Data sources are displayed in the **Import Data Source** section.

   If an error is encountered, then you need to review your CSV file to correct errors, and import the file again. If the data source list is structured incorrectly or the data source list contains incorrect information, import of the CSV file might fail.
8. Specify connection parameters to the data sources that are imported to establish connection to the database.

   a. Select a database and double-click.

   b. Set the following options and click **Add**.

Adapter	Data collector name.
Agents	Agent name to connect to the database.
Database Name	Name of the database.
Identifier	Name for the data source.
User Name	Name of the database user.
Password	Password for the database user name.

9. To view the data sources that you added, click **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**.

Application inventory

The IBM Data Risk Manager application inventory is constituted of applications, their attributes, and relations to other business entities. Use the Manage Inventory component to view and manage applications that you imported through CSV files as context data and their associations with other business entities such as data sources, hosted infrastructures, and business processes.

IBM Data Risk Manager provides visibility to information asset risks in the business context data of an organization. Viewing information asset risks requires an initial one-time capture and import of organizational business context data in terms of business units, lines of business (LOB), business processes, applications, and stakeholders.

Import the business context data into IBM Data Risk Manager by using one or multiple files in comma-separated values (CSV) format. You can then modify and add application context data based on your needs.

For more information about business context data, see "Mapping business context data" on page 99.

Viewing application inventory data

You can view and interact with application context data that is constituted of applications, their attributes, and relations to other entities.

Before you begin

To view and manage application inventory data, ensure that the business context data is imported into IBM Data Risk Manager. For more information about business context data, see "Mapping business context data" on page 99.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. To view list of applications, go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Application**.

   Along with the application name, you can also view application source information. For example, `ServiceNow`, `OneTrust`, `Native`, or `Registry`.

Application Source	Description
ServiceNow	Data is imported into IBM Data Risk Manager inventory from ServiceNow.
`OneTrust`	Data is imported into IBM Data Risk Manager inventory from OneTrust.
`Native`	Data is imported into IBM Data Risk Manager inventory by using CSV files.
`Registry`	Data is added to IBM Data Risk Manager application inventory by using the **Manage Inventory** component.

4. Select an application from the list to view its properties under **Property Details**.
5. To add an application to the inventory, click the **Application** icon ⊕.
6. For a selected application, you can run the following operations.
   - To modify application details, click the **Edit** icon ✎.
   - To delete an application from the inventory, click the **Delete** icon 🗑.
   - To associate other business entities with the application, click the **Connect** icon ⋖.
7. Click **Refresh Dashboard** for refreshing IBM Data Risk Manager Dashboard with the modified application context data in the published information assets.

Adding an application to inventory

Use the **Manage Inventory** > **Application** component of IBM Data Risk Manager to add application context data to the inventory.

About this task

IBM Data Risk Manager provides visibility to information asset risks in the business context data of an organization in terms of applications, business processes, business units, lines of business (LOB), and stakeholders. You can import application context data into IBM Data Risk Manager inventory through CSV files. To this inventory, you can add applications and their properties according to your business needs. For more information about business context data, see "Mapping business context data" on page 99.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Application**. The list of applications is displayed.
4. On the **Applications** window, click the **Application** icon ⊕.
5. On the **Application** window, set the following options.

Option	Description
Name	Specify a name for the application that you are adding to the inventory.
Display Name	Specify the display name of the application.
Description	Add a description for the application that you are adding.

6. To save the application details, click **Save**. Application that you added now is displayed in the list of applications. Along with application name, **Registry** indicates that the application is added to inventory by using the **Manage Inventory** component.
7. Define the application properties.
   a) Select the application that you now added from the list. The application properties are displayed in the **Property Details** window.

   These properties are imported from CSV files to IBM Data Risk Manager.

   b) Specify appropriate values to the properties.

   c) Click **Save**.

What to do next

Connect the application that you now added with other business entities. For more information about the connection, see "Associating applications with other business context entities" on page 118.

Associating applications with other business context entities

You can associate the applications that you added to inventory with appropriate business context entities such as data sources, hosted infrastructures, or business processes based on your requirements. You can also modify connection details of the existing applications that you imported by using CSV files.

About this task

For more information about business context data, see "Mapping business context data" on page 99.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).

2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Application**. The list of applications is displayed.
4. From the list, select an application that you want to associate with other business entities.
5. Click the **Connect** icon .
6. Connect the application with other business entities based on your business needs.

   Business processes

   a. Click **Business Process Mapping**.
   b. From the **All Business Processes** list, select business processes to associate with the application.
   c. Click the forward arrow icon →.

   Data sources

   a. Click **Datasource Mapping**.
   b. From the **All Data Sources** list, select data sources to associate with the application.
   c. Click the forward arrow icon →.

   Infrastructures

   a. Click **Hosted Server Mapping**.
   b. From the **All Hosted Servers** list, select servers to associate with the application.
   c. Click the forward arrow icon →.
7. If you want to cancel any of your selections, run the following steps.
   a) Choose items that you want to cancel from the selected list of business processes, data sources, or hosted servers.
   b) Click the backward arrow icon ←.
8. Click **Save Connection** to save the connection details.

Business process inventory

The IBM Data Risk Manager business process inventory is constituted of business processes, their attributes, and relations to other business entities. Use the Manage Inventory component to view and manage business processes that you imported through CSV files as context data and their associations with other business entity such as applications.

IBM Data Risk Manager provides visibility to information asset risks in the business context data of an organization. Viewing information asset risks requires an initial one-time capture and import of organizational business context data in terms of business units, lines of business (LOB), business processes, applications, and stakeholders.

Import the business context data into IBM Data Risk Manager by using one or multiple files in comma-separated values (CSV) format. You can then modify and add business process context data based on your needs.

For more information about business context data, see "Mapping business context data" on page 99.

Viewing business process inventory data

You can view and interact with business process inventory data that is constituted of business processes, their attributes, and relations to other entities.

Before you begin

To view and manage business process inventory data, ensure that the business context data is imported into IBM Data Risk Manager. For more information about business context data, see "Mapping business context data" on page 99.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. To view list of business processes, go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Business Process**.

   Along with the business process name, you can also view source information. For example, `Native` or `Registry`.

Business Process Source	Description
`Native`	Business process is imported into IBM Data Risk Manager inventory by using CSV files.
`Registry`	Business process is added to IBM Data Risk Manager inventory by using the **Manage Inventory** component.

4. Select a business process from the list to view its properties under **Property Details**.
5. To add a business process to the inventory, click the **Business Process** icon ⊕.
6. For a selected business process, you can run the following operations.
   - To modify business process details, click the **Edit** icon ✎.
   - To delete a business process from the inventory, click the **Delete** icon 🗑.
   - To associate other business entities with the process, click the **Connect** icon ⋔.
7. Click **Refresh Dashboard** for refreshing IBM Data Risk Manager Dashboard with the modified business process context data in the published information assets.

Adding a business process to inventory

Use the **Manage Inventory** > **Business Process** component of IBM Data Risk Manager to add business process context data to the inventory.

About this task

IBM Data Risk Manager provides visibility to information asset risks in the business context data of an organization in terms of applications, business processes, business units, lines of business (LOB), and stakeholders. You can import business process context data into IBM Data Risk Manager inventory through CSV files. To this inventory, you can add business processes and their properties according to your business needs. For more information about business context data, see "Mapping business context data" on page 99.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Business Process**. The list of business processes is displayed.
4. On the **Business Processes** window, click the **Business Process** icon ⊕.
5. On the **Business Process** window, set the following options.

Option	Description
Name	Specify a name for the business process that you are adding to the inventory.
Display Name	Specify the display name of the business process.
Description	Add a description for the business process that you are adding.

6. To save the business process details, click **Save**. Process that you added now is displayed in the list of business processes. Along with business process name, **Registry** indicates that the process is added to inventory by using the **Manage Inventory** component.
7. Define the business process properties.
   a) Select the business process that you now added from the list. The business process properties are displayed in the **Property Details** window.

   These properties are imported from CSV files to IBM Data Risk Manager.

   b) Specify appropriate values to the properties.

   c) Click **Save**.

What to do next

Connect the business process that you now added to other business entities. For more information about the connection, see "Associating a business process with other business entities" on page 121.

Associating a business process with other business entities

You can associate the business processes that you added to inventory with appropriate business context entity such as applications based on your requirements. You can also modify connection details of the existing business processes that you imported by using CSV files.

About this task

For more information about business context data, see "Mapping business context data" on page 99.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Business Process**. The list of business processes is displayed.
4. From the list, select a business process that you want to associate with other business entity such as application.
5. Click the **Connect** icon ⋔ .
6. Connect business process with the applications.
   a. Click **Application Mapping**.

b. From the **All Applications** list, select applications to associate with the business process.

c. Click the forward arrow icon →.

7. If you want to cancel any of your selections, run the following steps.

   a) Select applications from the **Selected Applications** list.

   b) Click the backward arrow icon ←.

8. Click **Save Connection**.

Threat inventory

The IBM Data Risk Manager threat inventory is constituted of possible threats on information assets and their properties. Use the Manage Inventory component to view and manage threat information.

Go to **IBM Data Risk Manager** > **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Threat** to view and manage threats.

Viewing threat inventory data

You can easily view and interact with threat inventory data that is constituted of threats, their properties, and the action plans.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. To view list of threats, go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Threat**.
4. To add a threat to the inventory, click the **Add** icon ⊕.
5. To modify threat details, select a threat from the list and click the **Edit** icon ✎.
6. To refresh threat inventory list, click the **Refresh** icon ⟳.

Adding a threat to inventory

You can define possible threats and their properties in IBM Data Risk Manager for risk analysis and actions.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Threat**.
4. On the **Threat** page, click the **Add** icon ⊕.
5. On the **Threat** window, set the following options.

Option	Description
Threat Name	Specify a name for the threat that you are adding to the inventory.
Threat Type	Select the threat type.
Category	Specify the threat category.

Option	Description
Threat Description	Add more information about the threat that you are adding.
Relative Weight	Assign a relative weight to the threat.
Impact	Specify the possible impact of the threat.
Probability	Specify the likelihood of threat occurrence.
Active	Enabled toggle button indicates that the threat is in active state.
Syslog	Enable the toggle button to specify details for creating the threat based on syslog alerts. a. Click **Next**. b. Specify details in the following fields. • **Number of Days** • **Duration** • **Threshold Range** • **IP Address** • **Specific Day of Week** • **Severity** • **Policies**

6. Click **Next**.
7. Select the appropriate remediation activities and the tasks.
8. Click **Save**.

Solution packages

IBM Data Risk Manager enables definition and development of specific policies and rules to address customer requirements for discovery and classification and controls integration. A set of pre-defined policies and rules is provided to address common customer requirements such as discovering personally identifiable information (PII). The solution packages for policies and rules, and their attributes can be customized based on the organizational context such as database platform, types, and naming conventions.

During the initial phase of a project, requirements for policies and rules are captured through interviews and workshops with key business and technical stakeholders. Based on specific customer requirements, the solution packages are customized and prepared in the required format. You can then import the solution packages IBM Data Risk Manager.

Importing solution packages

Use the Business Context Modeler component of IBM Data Risk Manager to import solution packages. The solution package contains a set of pre-defined policies and rules to address common customer requirements such as discovering personally identifiable information (PII).

Before you begin

Ensure that the solution packages are available for importing.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Solution Package**.
4. Click **Choose File** to load the files for **Solution Package**, **Policies**, and **Tasks**.

   Click the respective buttons to view contents in the preview section.
5. Click **Import** to import the solution packages.

What to do next

To verify whether the solution packages are successfully imported, go to **Business Context Modeler** > **Policy Managment Central**.

Managing programs

IBM Data Risk Manager program represents a discovery, classification, and controls integration effort that are defined for one or more business areas or line of business, organization groups, applications, business processes, and other organization-specific entities.

The IBM Data Risk Manager enable organizations to approach data security in a focused way by programmatically defining objectives and scope for a data discovery and classification initiative. Often, organizations embark on data discovery and classification in a large scale that contains many business areas, applications, and processes. In IBM Data Risk Manager, you can view data sources, both structured and unstructured, by different entities such as business areas, lines of business, applications, and business processes. Only relevant data sources can be included for the discovery and classification engagement, prioritizing on the most valuable or most suspect to contain critical data of the organization.

Scoping is an activity that sets or maps the boundaries or limits of the risk assessment to be conducted. Scoping must be carried out at an early stage of the project based on the information that is captured through interviews and workshops with the sponsors and key stakeholders.

Creating a program

Use IBM Data Risk Manager for creating a program to define and scope business information based on business areas, lines of business, applications, processes, and other organization business context metadata.

About this task

Consider the following factors to create programs and subprograms.

- Any number of subprograms or child programs can be created for a parent program.
- You can create a program as parent or a child program. By default, the program is created as a parent program. When the sub program option is selected, you must provide details of the parent program and save the sub program.
- When details of a program are displayed on the program portfolio page, the subprograms information is also displayed.
- When a parent program is selected, all its subprograms are also listed, if they are created.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.

3. Go to **Business Context Modeler** > **Home**.
4. On the **Program Portfolio** page, click the **Add Program** icon ⊕ to create a program.
5. Set the following options and click **Save**.

Option	Description
Name	Specify a name for the program.
Owner	Select a program owner from the list of users. To display the list, click the 👤 icon.
Description	Specify the additional information that indicates purpose of the program that you are creating.
Start Date	Specify the start date of the program.
End Date	Specify the end date of the program.

6. When the program is saved, the following message is displayed. Click **Yes** to assign a user, user group, and scope the program.

```
Program is saved successfully. Do you want to scope entitlements for the program?
```

7. Assign users, user groups, and scope the program. Then, click **Assign**.
   a) To assign users, select the users under **Users**. The assigned users can access data that is discovered according to scope of the program.
   b) To assign user groups, select the groups under **User Group**.
   c) To scope the program, select the necessary business context entities under **Scope**. The business context entities are imported from various sources.
   You can assign the following business context entities.
   - Line of Business (LOB)
   - Application
   - Platform
   - Compliance
   - Environment
   - Resource
   - Data Source

   Note: If the business context entities are not selected, scope of the program includes all the available data sources. Program scope is set to all-inclusive by default.
8. Click **Evidence** to create and associate an evidence with the program.

Managing policies

A policy is a set of operations that you want IBM Data Risk Manager to perform. Use IBM Data Risk Manager to define policies and associated rules for data discovery and classification, cleansing and analysis, and controls such as database activity monitoring.

Use **IBM Data Risk Manager Application Suite** > **Business Context Modeler** > **Policy Management Central** to define and deploy IBM Data Risk Manager policies. IBM Data Risk Manager contains the following types of policies.

- Policies that are created in IBM Data Risk Manager.
- Policies and rules that are imported through Solution Packages.

You can manage the following policies in IBM Data Risk Manager.

Data Discovery and Classification
IBM Security Guardium classification policies for data discovery.

Analysis Workbench Policy
IBM Data Risk Manager native analysis rules for information asset grouping.

Database Activity Monitoring (DAM)
IBM Security Guardium database activity monitoring policies for security policy violations.

You can deploy policies and rules on an application by using IBM Data Risk Manager Application Suite. For example, you can define IBM Security Guardium DAM policies in Policy Management Central, and then deploy on IBM Security Guardium systems such as Central Manager, Collector, or Aggregator based on their availability to IBM Data Risk Manager Server.

Creating an analysis workbench policy for structured data sources

You can create analysis workbench policies in IBM Data Risk Manager to define custom rules for creating information asset groups upon completing metadata scans on target structured data sources. The policies that are imported as part of the solution packages are available in analysis workbench to create information asset groups.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the menu icon ⠿.
3. Go to **Business Context Modeler** > **Policy Management Central**.
4. Click the **Select Policy Type** icon ▽ , and select **Analysis Workbench Policy**.
5. Click **Structured**.
6. To create an analysis workbench policy for structured data sources, click the **Add New Policy** icon 📋 on the **Details** section.
7. On **Cleansing Policy Builder**, set the following options to create a new policy.

Option	Description
Name	Specify the name of the analysis policy.
Description	Add a description for the analysis policy.
Rule Set Name	Specify the rule set name.
Category	Select the analysis policy category from the list.
Classification	Select the policy classification from the list.
Asset	Specify the asset name.

8. Click the **Add Rule** icon + to add a `Cleansing` rule.

   The analysis workbench rules can be used to define metadata patterns to run data matches on table names and column names.

Option	Description
New Rule Description	Specify the name of the rule.
Operations	Select the type of operation from the list that specifies conditions to perform a match for the rule.
Applied On	Include table details for a match.

Option	Description
Pattern	Specify exact match for a discovery pattern for a native analysis rule.
Synonyms	Specify multiple discovery patterns for a native analysis rule.

9. Create an additional rule to identify table and column names that contain a specific pattern or synonym.
10. Click **Save** to save the policy and rule details.

    The analysis policy can be used for information asset grouping for metadata scans that are performed by IBM Data Risk Manager.

Creating an analysis workbench policy for unstructured data sources

You can create analysis workbench policies in IBM Data Risk Manager to identify false positives and classify unstructured metadata on the target unstructured data sources.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the menu icon ⠿.
3. Go to **Business Context Modeler** > **Policy Management Central**.
4. Click the **Select Policy Type** icon ▽ , and select **Analysis Workbench Policy**.
5. Click **Unstructured**.
6. To create an analysis workbench policy for unstructured data sources, click the **Add New Policy** icon 📋 on the **Details** section.
7. On **Unstructured Policy Builder**, set the following options to create a new policy.

Option	Description
Name	Specify the name of the analysis policy.
Description	Add a description for the analysis policy.
Policy Label	Specify the policy label name
Asset Name	Specify the asset name.

8. Click the **Add Rule** icon + to add a rule.
9. Select a rule type under **Content Based** or **File Properties** according to the requirements.
10. Click **Next**.
11. Specify a name for the rule.
12. Specify the asset name.
13. Specify the other rule criteria for the selected rule type according to the requirements.
14. Create an additional rule under **Content Based** or **File Properties** according to the requirements.
15. Click **Save** to save the policy and rule details.

    The analysis policy can be used for information asset grouping for metadata scans that are run by IBM Data Risk Manager on unstructured data sources.

Modifying a policy

Policies that are defined on IBM Data Risk Manager Policy Management Central can be edited to add and update rules, parameters, and values to meet your requirements.

About this task

Note: Policies that are imported from IBM Security Guardium, and that are already deployed on IBM Security Guardium cannot be edited.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the menu icon ⠿.
3. Go to **Business Context Modeler** > **Policy Management Central**.
4. Click the **Select Policy Type** icon ⧩ to select a policy type to display the policies.
5. Select a policy to edit from the policy list.
6. Click the **Edit** icon ✎.
7. On the policy builder page, modify the policy details according to your requirements.

   To add a rule for the policy:

   a. Click the **Add Rule** icon + .
   b. Specify the rule definition according to your requirements.

   To edit a rule information for the policy:

   a. Select a rule from the list for editing.
   b. Click the edit icon ✎, and make the necessary changes.

   To remove a rule for the policy

   a. Select a rule from the list to delete.
   b. Click the delete icon 🗑.
8. Click **Save** to save the changes.

Cloning a policy

Use the IBM Data Risk Manager clone function to create a copy of an existing policy with a new name.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the menu icon ⠿.
3. Go to **Business Context Modeler** > **Policy Management Central**.
4. Click the **Select Policy Type** icon ⧩ to select a policy type to display the policies.
5. Select a policy that you want to clone from the policy list.
6. Click the **Clone** icon 🗐.
7. Click **Yes** on the confirmation dialog.
8. Specify a new name for the policy.
9. Click **OK** to clone the existing policy.

Removing a policy

You can delete policies from IBM Data Risk Manager if they are no longer needed.

About this task

Note: Policies that are imported from IBM Security Guardium, and that are already deployed on IBM Security Guardium cannot be deleted.

Procedure

1. Log in to IBM Data Risk Manager Application Suite with administrator privileges.
2. Click the menu icon ⠿.
3. Go to **Business Context Modeler** > **Policy Management Central**.
4. Click the **Select Policy Type** icon ▽ to select a policy type to display the policies.
5. Select a policy that you want to remove from the policy list.
6. Click the **Delete** icon 🗑.
7. Click **Yes** to remove the policy.

Security Command and Control Center dashboard

The Security Command and Control Center (SC3) dashboard, the landing page of IBM Data Risk Manager SC3 component, displays a graphical representation of data sources, information assets, status of security scan processes, and transaction details that are associated with the specified program and user. Graphical representation of data helps you to easily understand and interpret information.

The SC3 component of IBM Data Risk Manager is used to run data discovery scans on the defined data sources. Discovered data results are then used to analyze, filter, and categorize information assets.

The SC3 dashboard contains the following widgets.

- Security Scan Processes and Status
- Data Visualizer
- Information Assets / Data Sources

You can customize default colors of the widget elements with user-configured colors according to your requirements. For the steps on how to customize colors, see "Configuring color schemes for widget visualizations" on page 160.

Accessing SC3 dashboard

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) with your user credentials.
2. Click the menu icon ⠿.
3. Go to **Security Command and Control Center** > **Program**.
4. Select a program for which you want to view the data source and scan information and to run discovery and classification operations.

   The **Security Command and Control Center** > **Home** dashboard page is displayed.

Security Scan Processes and Status

The Security Scan Processes and Status widget provides a consolidated view of security scan processes and their status. You can view the following information.

- List of data classifier processes and their status ran in the last one month under **Recent Scans**. The list shows triggered and download processes of structured and unstructured data. Click the ••• icon on a scan process to view details of the associated data sources.
- List of vulnerability assessment processes and their status for triggered and downloaded processes under **Vulnerability Assessment Processes**. Click the ••• icon on a scan process to view details of the associated data sources.
- Shows cumulative percentage of data sources that are scanned for the last 6 months. Percentage is shown for the statuses such as **Completed**, **Failed**, **Scheduled**, **In Progress**, **Queued**, and **New**.
- Bar chart that shows number table counts of the data sources that are scanned in the last six months. In the chart, X - axis represents the timeline (month or day). If the scans are run for less than 60 days, the time is represented in days. If the scans are run for more than 60 days, the time is represented in months. Y - axis represents count of database tables (structured data of downloaded and triggered scans) and the files (unstructured data). Hover on a bar to view table counts for a specific timeline. Only the distinct count of tables in **Uncleansed** and **Tagged** data categories from **Analysis Workbench** page is shown. Count does not include the number of tables in the **Excluded** and **Exported** data categories. You can view the data based on **Transaction Types**, **Source**, and **Platform**. Click the bar to view the associated information under **Transaction Details**.

Data Visualizer

Data Visualizer is a visual representation of the data sources that are in scope, and which is overlaid with business metadata information. By default, the visualizer represents all the data sources based on Line of Business (LOB). When you click the **LOB** icon, the **Choose Items to Plot** list box is displayed if the items are more than 10. The visualization diagram is displayed in the Data Visualizer widget for the attributes you selected. To view drill-down details, run the following steps.

1. On the Data Visualizer widget, click the **Expand** icon ↗.
2. On the expanded Data Visualizer view, click the attribute icon of the diagram.

Run the following steps to configure the visualizer.

1. On the expanded Data Visualizer view, click the visualizer settings icon ⚙.
2. Make the necessary selection of attributes from the list.

In the expanded Data Visualizer view, click the **Collapse** icon ↙ to display the SC3 dashboard page.

Information Assets / Data Sources

Information Assets
: Shows information asset counts for the selected program in donut chart and in the list view for the statuses such as **Published** and **Under Review**.

Data Sources
: Shows data source counts for the selected program in donut chart, and also in the list view based on the data discovery scan results such as **Discovered**, **Failed**, **Yet to be Discovered**, and **Scheduled**.

Discovering data

Use the Security Command and Control Center (SC3) component of IBM Data Risk Manager to run data discovery scans on the defined data sources. Discovered data results are then used to analyze, filter, and categorize information assets.

The Data Ingestion Wizard (DIW) can be used to run the discovery processes based on defined policies and criteria by using job scheduling through IBM Security Guardium scanning or native metadata discovery scans. You can also import the classifier scans from IBM Security Guardium into IBM Data Risk

Manager for data analysis. Taxonomy definition and classification of discovered data elements are performed based on the analysis of metadata for the discovered information and data assets.

Running data discovery scan by using IBM Security Guardium

Use the Security Command and Control Center (SC3) component of IBM Data Risk Manager to run the IBM Security Guardium classifier scan.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security Guardium. For integration information, see "Integrating IBM Security Guardium with IBM Data Risk Manager" on page 36.

Ensure that the necessary business context data is imported, and the availability of a program with adequate scope to run the data discovery operation.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`) with administrator privileges.
2. Click the menu icon ⠿.
3. Go to **Security Command and Control Center** > **Program**.
4. Select a program in which you want to perform discovery and classification.

   The Data Visualizer is displayed on the **Security Command and Control Center - Dashboard** page.

   The Data Visualizer is a visual representation of the data sources that are in scope that is overlaid with business metadata information. You can configure the decomposition of the visualization tree by running the following steps.

   a. Click the menu icon ⚙.

   b. Select attributes from the drop-down list according to your requirements.

   c. Click **Done**.

   Depending on the configuration, you can see the drill-down details by double-clicking each node of the tree.
5. Go to **Security Command and Control Center** > **Inventory**.
6. Click the **Change Collector** icon ⇥.
7. Select **IBM Guardium**.
8. Select data sources from the **Data Source Inventory** list.
9. Select policies from the **Policy Inventory** list.
10. Click the **Trigger Scan Wizard** icon 👁.
11. Specify a name for the classification process.
12. According to your requirements, select the check boxes to include **User Tables**, **View**, or **System Tables** in the scan.

Running native metadata scanning

Use the Security Command and Control Center (SC3) component of IBM Data Risk Manager to run the IBM Data Risk Manager native metadata scan on structured and unstructured data sources.

Before you begin

Ensure that the necessary business context data is imported, and the availability of a program with adequate scope to run the data discovery scan.

To run a metadata scan on Oracle databases, user must have the permission to access database objects (dba_objects). Run the following command to provide access to the user.

```
grant create session, select any dictionary to <user_name>;
```

About this task

Following document formats are supported for unstructured scanning.

- HyperText Markup Language (HTML)
- Extensible Markup Language (XML)
- Microsoft Office document formats
- Portable Document Format (PDF)
- Rich Text Format (RTF)
- Compression and packaging formats
- Text formats
- Java class files
- Source code
- Log files
- Comma-separated values (CSV) files

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) with administrator privileges.
2. Click the menu icon .
3. Go to **Security Command and Control Center** > **Program**.
4. Select a program in which you want to perform discovery and classification.

   The Security Command and Control Center (SC3) dashboard is displayed. The dashboard displays a graphical representation of data sources, information assets, status of security scan processes, and transaction details that are associated with the selected program.
5. Click **Inventory**.
6. Click the **Change Collector** icon .
7. To run the scan on structured data sources, select **Native Structured**.
8. To run the scan on unstructured data sources, select **Native Unstructured**.
9. Select data sources from the **Data Source Inventory** list.
10. Select policies from the **Policy Inventory** list.

    Note: No policies for structured meta scanning.
11. Click the **Trigger Scan Wizard** icon .
12. Specify a name for the classification process in **Enter Classification Process Name**.
13. For structured data sources, specify the following details.

    a. According to your requirements, select the check boxes to include **User Tables**, **View**, or **System Tables** in the scan.

    b. Select **Enable Row Count** to display number of rows in the data source tables.
14. To start the scan immediately, select **Scan Now**.
15. To start the scan later, select **Scan Later** and specify the schedules.
16. To start the process, click **Trigger Metadata Scan**.

17. To view the scan status, go to **Security Command and Control Center** > **Home**.

Viewing data discovery scan results

Use the Security Command and Control Center (SC3) component of IBM Data Risk Manager to view the data discovery scan results for further analysis and actions.

Before you begin

View the completed scans along with the status. To view the status, go to **Security Command and Control Center** > **Home**.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`) with administrator privileges.
2. Click the menu icon .
3. Select a program from the list.
4. Go to **Security Command and Control Center** > **Analysis**.
5. Select the data source from **Database List** for which you need to review the scan results.
6. On the **Analysis Workbench** page, the tables and columns for the identified target database and appropriate matches if a policy was applied during classification scan are displayed.
7. Ensure that scans are completed for all the data sources, which are in scope against the policies that match the data source contents.

Importing classifier scans from IBM Security Guardium

You can import classifier scans from IBM Security Guardium appliances into IBM Data Risk Manager inventory for data classification and risk analysis.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security Guardium. For more information about integration, see "Integrating IBM Security Guardium with IBM Data Risk Manager" on page 36.

About this task

The transaction icon indicates that the previous import operation was successful.

The transaction icon indicates that the previous import operation was failed.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Scans**.
4. Import data scans.

   a) Click the **Download** icon .

   b) On the **Import** window, select **Classifier**.

   c) From the **Adapter** list, select **IBM Guardium**.

   d) From the **Instances** list, select an adapter instance. You can select up to three instances.

    e) Select the date from which you need to pull the scans from IBM Security Guardium.
    f) To import all the processes that are associated with the selected instances, click **Import**.
    g) To import only the IBM StoredIQ processes that you need from the selected instances, run the following steps.
        1) Click **Import with Process Selection**.
        2) Select the processes that you need to import from each adapter instance.
        3) Click **Import**.

5. On the **Data Scans** page, you can view the scans that you now imported.
6. To refresh data scan inventory list, click the **Refresh** icon ⟳.
7. Alternatively, to view scan results after the import operation, go to **Security Command and Control Center** > **Home**.

Data cleansing and analysis

Use the Security Command and Control Center (SC3) component of IBM Data Risk Manager for cleansing and analyzing the data discovery scan results.

IBM Data Risk Manager cleansing and analysis function include the following tasks.

- Viewing the discovery results.
- Applying the filtering rules.
- Exporting the results to taxonomy.

During the analysis of data discovery scan results, data is grouped into following categories.

Uncleansed
Lists all the schema, tables, and columns that are not analyzed (data discovery scan results).

Tagged
Lists tables and columns that are a result of applying one or more filtering policies and rules.

Excluded
Lists tables and columns that are excluded from further analysis of the data discovery scan results.

Exported
Lists tables and columns that are exported after the analysis, and is ready to publish.

Schema-based discovery

For databases such as Oracle, IBM Data Risk Manager provides schema-based discovery. When triggering the meta scan, you can select the needed schemas. Also, on the cleansing workbench, assets can be grouped based on the schema.

Delta discovery

If the same data source gets scanned for discovery, delta portion of the table that were deleted or added are visible on the cleansing workbench.

Downloading data cleans results

Before exporting the cleanse results to taxonomy, you can create a CSV file to include the cleanse results and download the file to a folder of your choice.

Applying filtering rules

Apply policies and rules to the selected database to include or exclude data sets for the analysis.

Before you begin

- Ensure that the necessary business context data is imported, and the availability of a program with adequate scope to run the data discovery operation.
- Ensure that the data discovery scans for the data sources that are in scope are complete.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`) with administrator privileges.
2. Click the menu icon ⠿.
3. Select a program from the list.
4. Go to **Security Command and Control Center** > **Analysis**.
5. Select the data source from **Database List** for which you need to review the scan results.

   When the data discovery results are loaded initially, all the data such as tables and columns are tagged as `Uncleansed`.

   If the discovery and classification processes are completed in IBM Security Guardium, by default, the results are tagged to the associated IBM Security Guardium policy.
6. Click **Add Rule**. The filtering policies, which are defined in Policy Management Central, are displayed.
7. Select a policy from the list.
8. To include the policy rules, select **Inclusion**.
9. To exclude the policy rules, select **Exclusion**.
10. To apply the filter based the policy that you selected, click **Apply Filter**.

    The matching items are displayed in the **Tagged** section on the **Analysis Workbench** page.
11. If you need to exclude the columns, apply an elimination rule to remove the data elements from your set. Modify the associated policy to include a rule for removing data elements. For information about how to modify a policy, see "Modifying a policy" on page 128.
12. Click **Level Count** to view the list of policies that are applied. You can revert to an earlier stage of cleansing, by removing the filters at each level.
13. Repeat the steps to apply appropriate policies and rules for inclusion or exclusion according to your analysis requirements.

What to do next

Export the filtered set of data elements for taxonomy assignment and publishing. For information about how to export the analysis results, see "Exporting data analysis results" on page 135.

Exporting data analysis results

Export the filtered set of data elements for taxonomy assignment and publishing.

Before you begin

Ensure that the following tasks are completed.

- Import of necessary business context data, and the availability of a program with adequate scope to run the data discovery operation.
- Data discovery scans for the data sources that are in scope.
- Cleansing and analysis of data discovery scan results.

Procedure

1. After applying the necessary filtering policy rules, ensure that matching items are displayed in the **Tagged** section on the **Analysis Workbench** page.

   Tables and columns for the selected database, and appropriate matches if a policy was applied during classification scan, are displayed for the analysis.

2. To export the filtered set of data elements, click the **Export to Taxonomy** icon ⇥.
3. When prompted, click **Yes** to export the data sets to taxonomy.
4. Click the **Exported** icon 245 to view the exported tables.

What to do next

Go to **Security Command and Control Center** > **Taxonomy** to validate whether the export operation is successful.

Taxonomy mapping and publishing

Use the Security Command and Control Center (SC3) component of IBM Data Risk Manager for applying a taxonomy to the cleansed data assets and publishing assets to IBM Data Risk Manager Dashboard. The dashboard enables information governance by providing visualization and management in a single, unifying console that depicts potential risks to sensitive business assets.

Taxonomy-mapping features

- You can export the newly discovered information asset across multiple programs.
- If multiple information assets exist in the associated data source on **Security Command and Control Center** > **Taxonomy** > **Newly Discovered Assets**, you can apply the same taxonomy attributes to all assets and publish the asset.
- Information assets that are published or are ready to publish to the dashboard can be rolled back by using the `Rollback` option. When you use the `Rollback` option, the assets are moved back to the cleansing wizard.

Taxonomy mapping

Use the Security Command and Control Center (SC3) component of IBM Data Risk Manager for applying a taxonomy to the cleansed data assets and publishing the assets to IBM Data Risk Manager Dashboard.

Before you begin

Ensure that the following tasks are completed.

- Import of necessary business context data, and the availability of a program with adequate scope to run the data discovery operation.
- Data discovery scans for the data sources that are in scope.
- Cleansing and analysis of data discovery scan results.
- Export of cleansed data assets.

About this task

- You can export the newly discovered information asset across multiple programs.
- If multiple information assets exist in the associated data source on **Security Command and Control Center** > **Taxonomy** > **Newly Discovered Assets**, you can apply the same taxonomy attributes to all assets and publish the asset.

- Information assets that are published or are ready to publish to the dashboard can be rolled back. When the **Roll Back** option is used, the assets are moved back to the cleansing wizard.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`) with administrator privileges.
2. Click the menu icon ⋮⋮⋮.
3. Select a program in which you want to map taxonomy.
4. Go to **Security Command and Control Center** > **Taxonomy** > **Structured**.
5. Click the drop-down icon ▾ and select **Newly Discovered Assets**.

   The cleansed data assets that are exported from **Security Command and Control Center** > **Analysis** > **Analysis Workbench** are displayed.
6. Select a data source from the list that you want to publish.
7. On the **Newly Discovered Assets** page, if the context data is imported, primary and secondary taxonomy attributes are already be mapped. You can change the attributes if necessary. For example, you can change the `Compliance` and `Category` attributes.

   Note: If the taxonomy attributes are not automatically mapped, validate the mapping in **Business Context Modeler**.
8. On the **Primary Attributes** section, you can use tags to identify a group of associated data assets. You can:

   a. Create tags to define your data asset groupings.

   b. Associate a data asset with more than one tag.

   To create a tag:

   a. Click the **Tag** drop-down list.

   b. In the **Add new tag name** field, specify a name for the tag.

   c. To save the tag, click the add icon ⊕.

   To apply tags to a data asset:

   a. Click the **Tag** drop-down list.

   b. Select tags from the list.
9. To make the asset as a Crown Jewel asset, enable the toggle button. Crown Jewel is a term that is used to represent the most valuable data asset within an organization.
10. Assign Confidentiality Integrity Availability (CIA) rating for evaluating information asset risk, 1 = low, 2 = medium, and 3 = high.
11. Click **Save** to save the changes, if any.
12. Select **Apply to All** to apply changes to all the discovered assets in the current data source.
13. Click **Roll Back** if you want to roll back an information asset that is ready to publish to the dashboard. The information asset is moved back to the cleansing wizard for making necessary changes.
14. Validate the data assets, and click **Export**.
15. From the **Export** list, select the programs to which you want to publish the assets.
16. Click **Export**.

    The information assets are displayed in the list of published assets under **Security Command and Control Center** > **Taxonomy** > **Information Assets**.
17. To apply a taxonomy to the unstructured data assets, go to **Security Command and Control Center** > **Taxonomy** > **Unstructured**.
18. Repeat the same steps to apply taxonomy and export assets to the dashboard as needed.

What to do next

Verify whether the asset that you exported is now visible in IBM Data Risk Manager Dashboard.

Using dashboard to view the exported asset data

Use IBM Data Risk Manager Dashboard to view and analyze data from the discovery and classification process. The dashboard enables information governance by providing visualization and management in a single, unifying console that depicts potential risks to sensitive business assets.

Before you begin

Ensure that the following tasks are completed.

- Import of necessary business context data, and the availability of a program with adequate scope to run the data discovery operation.
- Data discovery scans for the data sources that are in scope.
- Cleansing and analysis of data discovery scan results.
- Export of cleansed data assets.
- Applying a taxonomy to the cleansed data assets and publishing assets to IBM Data Risk Manager Dashboard. For more information about dashboard, see "IBM Data Risk Manager Dashboard" on page 164.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) with administrator privileges.
2. Click the menu icon ⠿.
3. Click **Dashboard**.
4. Select your program.
5. Click **Dashboard**.
6. On the **Information Asset Portfolio** page, click the arrow icon → on the asset to view the asset details.

   The **Asset Details** pop-over is displayed.

Modeler diagrams

You can use **IBM Data Risk Manager** > **Business Context Modeler** > **Modeler** component to create business context flow diagrams and data flow diagrams. Data flow diagrams provide a lifecycle view of data and its flow across key organization entities that are easier to understand by technical and nontechnical audiences.

Creating a modeler diagram

You can create a model diagram by using IBM Data Risk Manager Modeler component to better understand the relationships among various business entities of an organization, for example, business processes, applications, or infrastructure.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.

3. Go to **Business Context Modeler** > **Modeler**.
4. Select **Diagram**.
5. Click the **Create Diagram** icon .
6. On the **Create Diagram** window, set the following options and click **Create**.

Option	Description
Diagram Name	Name of the diagram.
Business Unit	Name of the business unit.
Owner	Name of the owner.
Program	The program that is associated with the diagram.
Diagram Type	Diagram type, such as `Business Context` or `Data Flow`.

   Note: The list of template is displayed, if available. You can select the template to create your model diagrams.

7. To select the context data entities, click the drop-down icon .
8. Select an entity from the list, for example, `Application`.

   The attributes for the selected context data entity are displayed under `Application`.
9. To create the diagram, drag and drop the necessary attributes on the diagram area according to your needs and preferences.
10. Connect the entities by using the appropriate connectors and drawing options that are available in the drawing toolbar.
11. Click the connecting link to add link text to describe the relation.
12. To save the diagram, click the **Save Diagram** icon .
13. Alternatively, you can automatically plot the diagram.

    a) On the drawing area, on the selected attribute, click the auto connection icon .

    b) Select the necessary attributes from the list to meet your needs.

    c) Click **Plot**.

    d) To save the diagram, click the **Save Diagram** icon .
14. To open an existing diagram, click the **Open Diagrams** icon .

Creating a template diagram

You can create template diagrams in by using the IBM Data Risk Manager Modeler component. A model diagram can be created based on the available templates.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) with your user credentials.
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Modeler**.
4. Select **Template**.
5. Click the create template icon .
6. On the **Create Template** window, specify the diagram name.
7. Click **Create**.

8. To select the context data entities, click the drop-down icon .
9. Select an entity from the list, for example, `Application`.

   The attributes for the selected context data entity are displayed under `Application`.
10. To create the template, drag and drop the necessary attributes on the diagram area according to your needs and preferences.
11. Connect the entities by using the appropriate connectors and drawing options that are available in the drawing toolbar.
12. Click the connecting link to add link text to describe the relation.
13. To save the template, click the **Save Template** icon .
14. Alternatively, you can automatically plot the template diagram.

    a) On the drawing pane, on the selected attribute, click the auto connection icon .

    b) Select the necessary attributes from the list to meet your needs.

    c) Click **Plot**.

    d) To save the template, click the **Save Template** icon .

What to do next

The templates that you created are listed on the Create Diagram window. You can select a template from the list to create your model diagrams. Steps on how to create a model diagram, see "Creating a modeler diagram" on page 138.

To open an existing template, click the **Open Templates** icon .

Action Center

IBM Data Risk Manager provides risk and vulnerability remediation workflow function, which can be used to define an action plan, send it to the owner and track it to closure.

After data security issues are identified and the level of remediation requirement is assessed, organizations need to follow a remediation management process to address and manage the issues. You can use the Action Center component of IBM Data Risk Manager to manage remediation action plans for identified vulnerabilities and risks. Remediation activities can be defined for the following items.

Data sources

In the Action Center component, you can create an activity for a specific data source from IBM Data Risk Manager inventory to remediate the identified issues. If the data sources are imported from ServiceNow, you can use ServiceNow for remediation management. For more information about how to create an activity, see "Creating a remediation activity" on page 142.

Vulnerability assessment test results

In the Vulnerability Management component, you can assign a set of failed vulnerability assessment test results as scope to create a remediation activity. For more information about activity creation, see "Creating an activity to remediate vulnerabilities" on page 45. You can later use Action Center to view and manage these activities.

Risks from assessment

In the Assessment component, you can create a remediation activity for assessment risks that are associated with scopes such as applications, business processes, or data sources. For more information about activity creation, see "Creating an action plan to remediate risks" on page 187. You can later use Action Center to view and manage these activities.

Predefined remediation activities

You can add predefined remediation activities and tasks that are imported from a solution package for defining action plans in Action Center. For more information about how to add predefined activities, see "Adding predefined activities and tasks" on page 144.

ServiceNow for remediation management

You can use IBM Data Risk Manager and ServiceNow integration to create, update, and, close ServiceNow incidents for the remediation activities that are created in Action Center.

IBM Data Risk Manager and ServiceNow integration is a two-way integration that provides the following functions:

- Publishes remediation activities that are created for ServiceNow data sources from Action Center to your ServiceNow instance as incidents.
- Automatically updates activity or incident status and other details in Action Center and also in ServiceNow. If an activity is closed in Action Center, the corresponding ServiceNow incident is also closed. If the incident is resolved in ServiceNow, the corresponding Action Center activity is also closed.

Viewing project and remediation activity details

Action Center Dashboard of IBM Data Risk Manager provides an overall view of the projects and activities under each project that are defined to manage remediation actions on identified risks and vulnerabilities.

About this task

In Action Center, you can also view and manage remediation activities for vulnerabilities that you created in the Vulnerability Management component and the risk remediation actions that are created in the Assessment component of IBM Data Risk Manager. In the dashboard, you can view the following information.

- List of projects for a selected program.
- List of activities under each project.
- A quick overall status of the activities.
- Easy navigation to the projects and activities for viewing details and to monitor the status.
- A consolidated view of activity and tasks comments.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Action Center** > **Program** to select a program.
4. On the dashboard page, under **Projects**, list of projects is displayed. Select a project from the list. The activities that are defined for the selected project are displayed.
5. To create an activity for a selected program under a project, click the **Add Activity** icon ⊕.
6. To add predefined activity for a project, click the predefined activities icon 🛠. Predefined activities for remediation are imported from the solution packages.
7. For a selected activity, you can run the following operations.
   - To modify activity details, click the edit icon ✎.
   - To view associated tasks, click the down arrow icon ⌄ under **Tasks**. You can modify the task status and add a comment to the task.

- To view associated scopes, click the down arrow icon under **Scope**.
- To modify activity status, click the down arrow icon under **Status**. If you change the activity status to **Completed**, statuses of the associated tasks are also updated to **Completed**.
- To view and post a comment, click the comments icon . The **Activity Comments** widow provides a consolidated view of activity comments and task comments.
- To display activities on dashboard based on the selected criteria, click the filter icon for **Activity Name** or **Status**.

Creating a remediation activity

Use the Action Center component of IBM Data Risk Manager to create a remediation activity on identified vulnerabilities in a specific data source.

Before you begin

For a ServiceNow data source, you can create an activity and publish it as an incident on ServiceNow for remediation management. Currently, you can publish the activity only on a single instance of ServiceNow.

To use ServiceNow for remediation management, ensure that IBM Data Risk Manager is integrated with ServiceNow. For more information about integration, see "Integrating ServiceNow with IBM Data Risk Manager" on page 69.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Action Center** > **Program** to select a program.
4. On the dashboard page, click the **Add Activity** icon .
5. On the **Create Activity with Project** window, specify a project name and activity name. You can also select an existing project and specify an activity name.
6. To create a vulnerability remediation activity, click the **Remediation for Vulnerability Assessment** icon .
7. On the **Activity for Vulnerability Assessment** page, specify the necessary values for **Primary Fields**.

Option	Description
Status	Specify the activity status, for example, `Yet to Start`, `In Progress`, or `Completed`.
Select Data Source	Select a data source from the data source inventory for which you need create a remediation activity. You can assign only one data source as scope to an activity.
Publish In	If you select ServiceNow data source, you can publish the activity as an incident on ServiceNow. To publish, enable the ServiceNow toggle button. After the activity is published, you can view the incident number on the dashboard page.
Activity Operation	Select an operation activity from the list.
Start Date	Specify the date to start the remediation activity.
End Date	Specify the date to end the remediation activity.

Option	Description
Duration	Specifies the duration between activity start and end date.

8. Specify necessary values for **Secondary Fields**.

   You can add list items to the secondary fields such as **Impact**, **Urgency**, **Priority**, **Sub Category**, **Severity**, **Category**, and **Contact Type** by creating a register item for the respective registers (fields) in **Business Context Modeler** > **Framework Builder** > **Register Definitions**. You can add property to a register item to map IBM Data Risk Manager field with the equivalent ServiceNow field.

   For the steps about how to create a register item and to add a property, see "Creating an item and subitem for the register" on page 174.
9. To save the activity details, click **Save**.

What to do next

Define necessary context information to the activity that you now created. Click **Context Management** to define context information. For more information about context management, see "Defining context information for an activity" on page 143.

Defining context information for an activity

For the remediation activity that you created, add appropriate context information that helps you to better understand the activity.

About this task

You can define the following context information.

Activity Scope
: Failed results of vulnerability assessment scan that is run on the selected data source are available for assigning them as scope to the activity.

Tasks
: Tasks describe work items that are necessary to reach the aim of a remediation activity. Tasks have one or more task respondent users who are responsible to run the task within the specified timeframe. An activity can contain multiple tasks.

Notifications
: Notifications enable users to receive timely notice of activities and tasks. Multiple users can be notified.

Comment
: Comments provide a place to add any text to your activity. Comments might be often extra information, clarifications, opinions, details, or reviews.

Procedure

1. Create an activity under a project for the program that you select. For the steps on how to create an activity, see "Creating a remediation activity" on page 142.
2. On the **Activity for Vulnerability Assessment** page, click the **Context Management** icon ◉ .
3. Assign scope to the activity.
   a) Click **Activity Scope**.
   b) Select the necessary vulnerability assessment failed results as activity scope.
   c) Click **Save**.
4. Create a task. You can create multiple tasks for a remediation activity.
   a) Click **Tasks**.
   b) Set the following options and click **Save**.

Option	Description
Task Name	Specify a name for the task.
Task Operation	Select a task operation from the list.
Status	Specify the current task status, such as, `Yet to Start`, `In Progress`, or `Completed`.
Start Date	Specify the date to start the task.
End Date	Specify the date to end task.
Assigned Resources	Assign resources to run the task. You can select multiple resources.
Description	Add more information for the task that you create.
Comment	Add comments about the task.

5. Add notifications.
    a) Click **Notifications**.
    b) Set the following options and click **Save**.

Option	Description
Notification Name	Specify a name for the notification.
Status	Specify the notification status to indicate whether the notification is sent to the user.
Start Date	Specify the start date.
End Date	Specify the end date.
Assigned Resources	Assign resources to receive the notification. You can select multiple resources.
Description	Add more information about the notification that you are sending.
Comment	Add comments your comments about the notification.

6. Add a comment for the activity that you created.
    a) Click **Comment**.
    b) Add your comments.
    c) Click **Post**.
    d) Click **Save**.
7. You can view the activity that you now created with its associated context information in the Activity Center dashboard page.

Adding predefined activities and tasks

You can use predefined remediation activities and tasks that are imported from a solution package for defining action plans in Action Center.

Before you begin

Ensure that the solution packages are imported into IBM Data Risk Manager to use predefined activities and tasks. For more information about solution package, see “Solution packages” on page 123.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Action Center** > **Program** to select a program.
4. On the Action Center dashboard page, select a project from the **Projects** list.
5. Click the predefined activities icon 🛠.
6. On the **Predefined Activities for Remediation** window, select the necessary activities.
7. Click the **Add Activity** icon ⊕.
   Activities that you added are listed on the dashboard page.
8. Modify activity details based on the requirements. To modify activity details, select an activity and click the edit icon ✎.

Reporting

Use the IBM Data Risk Manager reporting function to generate reports and use them for business and analytical purposes.

Data protection requires continuous monitoring and analysis of data. IBM Data Risk Manager collects a large amount of data from multiple sources for risk analysis. You can view this data in the form of reports in various formats to easily view and analyze data. The IBM Data Risk Manager Reporting Engine is used to generate reports by using predefined templates for assets, inventory, assessment, and analysis workbench. Customized reports can be created by selecting columns, applying filters, and sorting order in which the column fields appear in the report, to meet your business needs.

Reporting templates

IBM Data Risk Manager provides the following report templates for creating your report.

- List of Asset with Infrastructure
- List of Information Assets with Data Assets
- List of Information Assets
- Infrastructure Inventory

For more information about IBM Data Risk Manager reporting templates, see “Reporting templates” on page 145.

Report formats

The generated report data is displayed in tabular format. You can then download this data to a comma-separated values (CSV) file. Download report to save the report data on your hard disk, perform further analysis, or to publish the report in a different application.

Reporting templates

Reporting templates are the pre-defined templates for different modules in the application. IBM Data Risk Manager report templates enable you to create your own reports with the metrics and data that you want to see.

IBM Data Risk Manager provides various templates as described in the following sections for creating your reports that help you analyze data and take informed business decisions.

List of Asset with Infrastructure

Report template provides details of IBM Data Risk Manager information assets and the associated infrastructures. You can use the template to showcase details of the Information Asset Portfolio and Infrastructure widgets of IBM Data Risk Manager Dashboard for a selected program.

Template elements	Description
Asset ID	System-generated unique asset identifier.
Asset Name	Name of the information asset.
Infrastructure Name	Name of the infrastructure.
Infrastructure ID	System-generated unique infrastructure identifier.
Infrastructure Risk Level	Risk level of the infrastructure. For example, High (red), Medium (amber), or Low (green) based on pre-defined scoring criteria.
Asset Risk Level	Risk level of the information assets. For example, High (red), Medium (amber), or Low (green) based on pre-defined scoring criteria.
Infrastructure City Location	Name of the city where the data source is located.
Infrastructure Country Location	Name of the country where the data source is located.
Table Count	Total number of data source tables that are associated with the information asset.
Infrastructure Classified Count	Total number of infrastructures that are associated with the information asset.
Crown Jewel	Indicates whether the information asset has Crown Jewel information of greatest value and would cause major business impact if compromised.
IP Address	Server IP address where the data source resides.
Host Name	Server host name of the data source.
Infrastructure Vulnerability Count	Total infrastructure vulnerability count that is associated with the endpoints or servers.
Asset Category	Data classification categories in terms of its need for protection such as Publicly Available, Internally Controlled, PII Confidential, Company Confidential, Highly Confidential/Restricted, Highly Confidential/Restricted, Public, Official Use Only, or Confidential.
Asset Compliance	Regulatory obligations that are associated with the asset such as HIPAA, SOX, or PCI.
Column Count	Total number of data source table columns that are associated with the information asset.
Program Name	Program name that the information asset is associated with.
Compliance	Regulatory obligations that are associated with the asset such as HIPAA, SOX, or PCI.
Sensitivity	Confidentiality Integrity Availability (CIA) rating for representing sensitivity level of information assets such as 1 = low, 2 = medium, and 3 = high.
Tag	Tag name that identifies a group of associated information assets.

List of Information Assets with Data Assets

Report template provides details of IBM Data Risk Manager information assets and the associated data assets. You can use the template to showcase details of the Information Asset Portfolio widget of IBM Data Risk Manager along with data of Overview section of the Information Asset Portfolio secondary page for a selected program.

Template Elements	Description
Classified Name	Name of the data source tables that is associated with the information asset.
Classified Column	Table column names of the data source that is associated with the information asset.
Asset ID	System-generated unique asset identifier.
Asset Name	Name of the information asset.
Infrastructure Name	Name of the infrastructure that is associated with the information asset.
IP Address	Server IP address where the data source resides.
Host Name	Server host name of the data source.
Tag	Tag name that identifies a group of associated information assets.
Program Name	Program name that the information asset is associated with.
Crown Jewel	Indicates whether the information asset has Crown Jewel information of greatest value and would cause major business impact if compromised.
Sensitivity	Confidentiality Integrity Availability (CIA) rating for representing sensitivity level of information assets such as 1 = low, 2 = medium, and 3 = high.
Compliance	Regulatory obligations that are associated with the asset such as HIPAA, SOX, or PCI.

List of Information Assets

Report template provides details of IBM Data Risk Manager information assets. You can use the template to showcase details of the Information Asset Portfolio widget of IBM Data Risk Manager Dashboard for a selected program.

Template Elements	Description
Name	Name of the information asset.
ID	System-generated unique asset identifier.
Category	Data classification categories in terms of its need for protection such as Publicly Available, Internally Controlled, PII Confidential, Company Confidential, Highly Confidential/Restricted, Highly Confidential/Restricted, Public, Official Use Only, or Confidential.
Type	Data asset type, for example, Information Asset.
Crown Jewel	Indicates whether the information asset has Crown Jewel information of greatest value and would cause major business impact if compromised.
Sensitivity	Confidentiality Integrity Availability (CIA) rating for representing sensitivity level of information assets such as 1 = low, 2 = medium, and 3 = high.
Compliance	Regulatory obligations that are associated with the asset such as HIPAA, SOX, or PCI.

Template Elements	Description
Risk Level	Risk level of the information assets. For example, High (red), Medium (amber), or Low (green) based on pre-defined scoring criteria.
Risk Reason	Reasons for the risk levels of the information assets.
Tag	Tag name that identifies a group of associated information assets.
Program Name	Program name that the information asset is associated with.

Infrastructure Inventory

Report template provides details of IBM Data Risk Manager data source inventory.

Template Elements	Description
Infrastructure Name	Data source name in the IBM Data Risk Manager inventory.
Platform	Database server name in which you created the data source.
IP Address	Server IP address where the data source resides.
Host	Server host name of the data source.
Total Table Count	Total number of data source tables.
Row Count	Row count of the table.
Total Asset Count	Total number of information assets to which the data source is associated.
City	Name of the city where the data source is located.
Country	Name of the country where the data source is located.
Classified	Security classification of the information assets.
Infrastructure with Crown Jewel	Indicates whether the information asset has Crown Jewel information of greatest value and would cause major business impact if compromised.
Infrastructure with Sensitive Data	Indicates whether the asset has sensitive data. Sensitivity level of data assets is represented by providing Confidentiality Integrity Availability (CIA) rating such as 1 = low, 2 = medium, and 3 = high.
Vulnerability Pass Count	Number of passed vulnerability scans.
Vulnerability Fail Count	Number of failed vulnerability scans.
Monitored	Indicates whether the database activities are monitored.
Encrypted	Shows Encryption status of the data sources. You must configure IBM Data Risk Manager to connect and interact with IBM Multi-Cloud Data Encryption to fetch encryption details of data sources that are added to the inventory from various sources where IBM Multi-Cloud Data Encryption agent is deployed for data encryption.
Violation Count	Number of policy violation count for the infrastructure.
Created Source	Name of the source in which the data source is created. For example, ServiceNow.

Creating and saving reports

Use the IBM Data Risk Manager reporting function to create reports by defining a set of instructions for extracting particular information to help you quickly view and analyze data.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Click **Report**.
4. Click the **New Report** icon ⊕.
5. On the **Create Report** page, select a template for your report.
6. Click **Next**.
7. Under **General Settings**, specify report name and description in the **Name** and **Description** fields.
8. Click **Next**.
9. Under **Table Settings**, run the following steps.
   a) Click **Select Columns** to add columns to the report. Column names are displayed based on the report template that you selected.
   b) Click the **Apply Filter** for selecting column to filter the report data.
   c) Click **Sort Columns** to define sort order of the applicable column fields in the report. You can sort the columns in **Ascending** or **Descending** order.
10. To save the report, click **Save Report**.

    The report that you saved is listed under the **Global Report List** section for later access.
11. Alternatively, click **Run Now** to save and immediately view report data.

What to do next

You can run the report later and view report data in tabular format, which can be exported to a CSV file. For the steps on how to run a report, see “Running a saved report” on page 149.

Running a saved report

When required, you can run your saved report definitions for viewing report data. If the report contains parameters, you can set values that you are interested in each time you run the report.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`) by using your credentials.
2. Click the application menu icon ⠿.
3. Click **Report**.
4. Under the **Global Report List** section, select the report that you want to run.
5. Click **Run Now** icon ⊡.
6. In the **Select Parameters** window, select parameters for the attributes that you selected for filtering report data.
7. Click **Run**.

   The generated report data is displayed in tabular format. You can then export the data to a CSV file.

What to do next

You can export the report data to a CSV file. For the steps on how to export report data, see "Downloading report data to a CSV file" on page 150.

Downloading report data to a CSV file

The generated report data is displayed in tabular format. You can then download this data to a comma-separated values (CSV) file. Download report to save the report data on your hard disk, perform further analysis, or to publish the report in a different application.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) by using your user credentials.
2. Click the application menu icon ⠿.
3. Click **Report**.
4. Select the report that you want to download from **Global Report List**. By default, the last executed report data is displayed in tabular format.

   To select a previously run report, run the following steps.

   a. Click the **Report Execution History** icon 🕓. The list of previously run reports is displayed.

   b. Select a report from the list.
5. To download report data to a CSV file, click the **Download Report** icon ⤓.
6. To open the file and save it to the folder of your choice, click the downloaded CSV file name that is displayed in lower left corner of the page.

Editing reports

You can modify the reports that are generated in IBM Data Risk Manager. For example, you might need to add new columns and filtering conditions for the report to suit your business needs.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) by using your user credentials.
2. Click the application menu icon ⠿.
3. Go to **Report**.

   Reports that are saved are listed under **Global Report List**.
4. Under the **Global Report List** section, select the report that you want to edit.
5. Click **Edit** icon ✎.
6. Make the necessary changes.
7. Click **Save Report**.

IBM Data Risk Manager Scheduler

Use the IBM Data Risk Manager Scheduler function to create and manage jobs for automatically running various transactions at the intervals that you define.

Job is a time-based scheduler that runs the predefined tasks on the server at a particular instance without the need of admin interference. Running the scheduled jobs keeps data in the IBM Data Risk Manager server in sync with the integrated server data. With IBM Data Risk Manager Scheduler, you can create scheduled jobs to run the following processes.

Load Vulnerability Assessment Scans

Transaction for creating the scheduled jobs to download vulnerability assessment scans from the integration adapter that you specify. For example, you can download vulnerability assessment scans from IBM Security Guardium, IBM QRadar Security Intelligence Platform, and IBM Security AppScan Enterprise.

Load Vulnerability Assessment Scan Results

Transaction for creating the scheduled jobs to download vulnerability assessment scan results from the integration adapter that you specify. For example, you can download vulnerability assessment scan results from IBM Security Guardium Analyzer.

Get Monitoring Status

Transaction for creating the scheduled jobs to get monitoring status of the infrastructure node. For example, you can get monitoring status of the infrastructure nodes from IBM Security Guardium and IBM Multi-Cloud Data Encryption.

Get Inventory and Risks

Transaction for creating the scheduled jobs to import inventory data and risks from the integration adapter that you specify. For example, you can import inventory data and risk information from OneTrust.

Viewing transaction and job details

The **Scheduler Console** page provides an overall view of the scheduled jobs that are defined for various transactions.

About this task

You can obtain and view the following details.

- List of transactions and the associated scheduled jobs.
- A quick overall status of the scheduled jobs.
- Easy navigation to the transactions and jobs for viewing details and monitor the status.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Scheduler**. The **Scheduler Console** page is displayed.
4. Under **Transaction List**, list of transactions is displayed. Select a transaction from the list. The scheduled jobs that are defined for the selected transaction are displayed under **Job Details** for viewing details.
5. To add a job, click the **Add Job** icon ⊕.
6. For a selected job, you can run the following tasks.

- To modify job details, click the **Edit** icon .
- To delete a job, click the **Delete** icon .
- To view the job run history, click the **History** icon .
- To enable or disable a job, click the toggle button .

Adding a scheduled job

Add jobs to run various transactions automatically at predefined intervals. For example, adding jobs for downloading vulnerability assessment scans, downloading vulnerability assessment scan results, getting monitoring status of infrastructure nodes, or importing inventory data and risks.

Before you begin

Ensure that IBM Data Risk Manager is integrated with the integration server from which you need to import data. For integration configuration details, see "Cross-product integrations" on page 32.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Go to **Business Context Modeler** > **Scheduler** .
4. Under **Transaction List**, select a transaction for which you need to add a job.
5. On the **Scheduler Console** page, click the **Add Jobs** icon ⊕.
6. On the **Create Job** window, set the following options.

Option	**Description**
Job Name	Specify a name for the job that you are adding.
Adapters	Specify the integration adapter instance name from which the data to be imported.
Job Parameters	For IBM Security Guardium instances, specify the date for **Start Date** parameter. Select **Updateable** to increment the date parameter for each run.

7. Click **Next**.

What to do next

You must define schedules to the job that you added. For the steps on how to configure the schedule, see "Configuring a scheduled job" on page 152.

Configuring a scheduled job

Scheduled jobs run automatically on a fixed interval on the server. You can define schedules for the jobs that are created by using IBM Data Risk Manager Scheduler.

Before you begin

Ensure that the job is created in IBM Data Risk Manager Scheduler.

When you are creating a job by using IBM Data Risk Manager Scheduler, schedules of the jobs are compared with the schedules of existing jobs of similar types. You must consider the following conditions for scheduling a job.

Load Vulnerability Assessment Scans

Start time of the new job cannot be between 60 minutes before and after the existing job start time. For example, if an existing scan download job is scheduled to run at 3 AM, you must schedule the new job to run before 2 AM or after 4 AM.

Load Vulnerability Assessment Scan Results

Start time of the new job cannot be between 60 minutes before and after the existing job start time.

Get Monitoring Status

Start time of the new job cannot be between 60 minutes before and after the existing job start time.

Get Inventory and Risks

Start time of the new job cannot be between 60 minutes before and after the existing job start time.

Procedure

1. Create a job. For the steps on how to create a job, see "Adding a scheduled job" on page 152.
2. Scheduled jobs can be set up to run by minute, every hour, every day, every week, every month, or any combination of these options. On the **Schedule** window, define the date and time of job execution according to your business needs.
3. Click **Save**.

   The job that you added is displayed on the **Job Details** page.

Vulnerability Management

You can use the Vulnerability Management component of IBM Data Risk Manager to create and trigger a scan to help you effectively identify vulnerabilities in your databases, endpoints, and applications. After scans identify vulnerabilities, you can search and review vulnerability data, remediate vulnerabilities, and rerun scans to evaluate the new level of risk.

Creating and triggering vulnerability assessment scan

Use the Vulnerability Management component of IBM Data Risk Manager to create and run the assessment scan in IBM Security Guardium to identify vulnerabilities in databases.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security Guardium. For more information about integration, see "Integrating IBM Security Guardium with IBM Data Risk Manager" on page 36.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Click **Vulnerability Management**.
4. Select a program from the list.
5. Click **Create New Assessment**.
6. On the **Create New Assessment** page, set the following options and click **Create Assessment**.

Option	Description
Assessment Name	IBM Security Guardium vulnerability assessment name.
Scan Type	Scan type, for example, `Database Scanner`.
Platform	Database type selection for running the vulnerability assessment process.

Option	Description
Run on	IBM Security Guardium adapter instance for running the vulnerability assessment process. List contains only the instances for which option **Run VA** is selected when the integration instance is created.

7. Under **Scope of Assessment**, add data sources to the transaction based on the scope or last scan days. You can add multiple data sources.
8. Click **Add Scope to Transaction**.
9. Select vulnerability tests from the list and click **Save**.
10. Under **Pending Transactions** on the Transaction View, click the **Start Process** icon .
11. Select **Scan Now**.

    To schedule the scan later, select **Scan Later**.

    To save transaction details after completion of the process under **Pending Transactions** for reuse, select **Replica**.
12. To start the process, click the **Trigger Assessment** icon .

Creating and triggering an endpoint assessment scan

Use the Vulnerability Management component of IBM Data Risk Manager to create and run the assessment scan in IBM QRadar Security Intelligence Platform to identify endpoint vulnerabilities.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM QRadar Security Intelligence Platform. For more information about integration, see "Integrating IBM QRadar Security Intelligence Platform with IBM Data Risk Manager" on page 50.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Click **Vulnerability Management**.
4. Select a program from the list.
5. Click **Create New Assessment**.
6. On the **Create New Assessment** page, set the following options and click **Create Assessment**.

Option	Description
Assessment Name	IBM QRadar Security Intelligence Platform endpoint assessment name.
Scan Type	Scan type, for example, `Server Vulnerability Scanner`.
Run on	IBM QRadar Security Intelligence Platform adapter instance for running the vulnerability assessment process.

7. Under **Scope of Assessment**, add data sources to the transaction based on the scope or last scan days. You can add multiple data sources.
8. Click **Add Scope to Transaction**.
9. Under **Pending Transactions** on the Transaction View, click the **Start Process** icon .
10. Select **Scan Now**.

To schedule the scan later, select **Scan Later**.

To save transaction details after completion of the process under **Pending Transactions** for reuse, select **Replica**.

11. To run the process, click the **Trigger Assessment** icon .

Creating and triggering an application assessment

Use the Vulnerability Management component of IBM Data Risk Manager to create and run the assessment scan in IBM Security AppScan Enterprise to identify application vulnerabilities.

Before you begin

Ensure that IBM Data Risk Manager is integrated with IBM Security AppScan Enterprise. For integration information, see "Integrating IBM Security AppScan Enterprise with IBM Data Risk Manager" on page 57.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Click **Vulnerability Management**.
4. Select a program from the list.
5. Click **Create New Assessment**.
6. On the **Create New Assessment** page, set the following options and click **Create Assessment**.

Option	Description
Assessment Name	IBM Security AppScan Enterprise application assessment name.
Scan Type	Scan type, for example, `Application Scanner`.
Run on	IBM Security AppScan Enterprise adapter instance to run the assessment process.

7. Under **Scope of Assessment**, add data sources to the transaction based on the scope or last scan days. Only one data source can be added to the transaction scope.
8. Click **Add Scope to Transaction**.
9. Select vulnerability test from the list and click **Save**.
10. Under **Pending Transactions** on the Transaction View, click the **Start Process** icon .
11. Select **Scan Now**.

    To schedule the scan later, select **Scan Later** and specify time to run the scan.

    To save transaction details after completion of the process under **Pending Transactions** for reuse, select **Replica**.

12. To start the process, click the **Trigger Assessment** icon .

Viewing scan results

Use the Vulnerability Management component of IBM Data Risk Manager to view vulnerability assessment scan results for further analysis and actions. Reviewing the data helps to identify issues that you can address to improve your organization's security posture.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).

2. Click the application menu icon .
3. Click **Vulnerability Management**.
4. Click **Results View**.
5. Click the filter icon under **VA Data Sources**, and select an adapter type, for example, `IBM QRadar`.
6. For a selected data source, click the number for **Pass**, **Fail**, or **Others** to display results in the **Vulnerabilities Test Results** page.

Creating an activity to remediate vulnerabilities

Use the Vulnerability Management component of IBM Data Risk Manager to view and remediate vulnerabilities. When the vulnerabilities are identified through scans, remediation actions must be taken to evaluate the correct risk exposure for the information asset.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon .
3. Click **Vulnerability Management**.
4. Go to **Results View**.
5. Click **VA Data Sources**.
6. Click the filter icon under **VA Data Sources**, and select your adapter type, for example, `IBM QRadar`.
7. Alternatively, you can select a data source based on the platform.
   a) Click **VA Platforms**.
   b) Select a platform and click the database icon to select your data source.
8. For a selected data source, click the number for **Fail** to display results in the **Vulnerabilities Test Results** page.
9. Click the down arrow icon to select the severity level.
10. Click the **Remediation** icon .
11. Click **Yes** to create remediation actions.
12. On the **Create Remediation Activity** window, specify the necessary information. If the data source is from ServiceNow, you can publish the activity as an incident on ServiceNow for remediation management.
13. Click **Create**.

    On the **Vulnerabilities Test Results** page, under **Activity**, you can view activity details if the end date of activity is greater than the execution date of test results.

What to do next

You can view and manage the remediation activities that you defined in the following areas.

IBM Data Risk Manager Action Center

- Click the application menu icon .
- Click **Action Center**.

For more information about Action Center, see "Action Center" on page 140.

Asset Details window on IBM Data Risk Manager Dashboard

- Click the application menu icon ⠿.
- Click **Dashboard**.
- On the **Information Asset Portfolio** window, click the arrow icon → on the asset to view the asset details.
- On the **Asset Details** window, click **Infrastructure** > **Vulnerabilities**.
- To view action items, select the infrastructure node and click **Action Items**.

Risk modeling and visualization

Use IBM Data Risk Manager to evaluate risks that are associated with sensitive data assets of an organization. You can then visualize the risks in IBM Data Risk Manager Dashboard to take necessary actions to protect your business.

IBM Data Risk Manager evaluates risk based on a combination of intrinsic nature of the data assets, and various infrastructure risk vectors. The intrinsic nature of the data assets refers to any applicable properties such as sensitivity of the data assets, classification level of the data assets, or whether a data asset has special characteristics, such as association with legal or policy-based obligations. Infrastructure vectors refer to vulnerabilities, events, and assessment risks that are associated with an infrastructure, which holds data assets.

Risk levels

IBM Data Risk Manager uses a three-point scale while assessing risks.

`High` [Red]	If a data asset is evaluated as `High` risk, the chances of breach or magnitude of potential breach is high. Immediate corrective actions are needed.
`Medium` [Amber]	If a data asset is evaluated as `Medium` risk, the chances of breach or magnitude of potential breach is medium. Corrective actions are needed within a reasonable period of time.
Low [Green]	If a data asset is evaluated as being at Low risk, the chances of breach or magnitude of potential breach is low. Corrective actions are not needed.

Risk factors and scoring

The risk factors and the telemetry data that is associated with risk factors are accumulated in a manner, which can be assimilated by IBM Data Risk Manager Risk Analytic Engine.

IBM Data Risk Manager considers factors that are described in the following sections to automatically evaluate information asset risk in a selected program.

Risks due to inherent attributes of data asset

In IBM Data Risk Manager, the following attributes determine inherent value of the data assets. A composite scoring of the attributes forms the basis to determine information asset risks.

Crown jewel
Represents the most valuable data asset within an organization. Typically, an organization possesses not more 2% of the total volume of data.

Category
Represents the data asset categories that are defined in IBM Data Risk Manager.

- Publicly Available
- Internally Controlled
- PII Confidential
- Company Confidential
- Highly Confidential/Restricted
- Public
- Official Use Only
- Confidential

Compliance
Represents regulatory obligations that are associated with the data asset.

Sensitivity level
Indicates the confidentiality, integrity, and availability requirements for the data asset.

Infrastructure risks

Infrastructure risk is an indication of security posture of the underlying infrastructure platforms. The data assets are located in infrastructure elements such as databases or file servers.

The following risk vectors are considered to calculate infrastructure risks.

Enforcement risks
Enforcement risks of the infrastructure are evaluated based on the following controls.

- Encryption
- Monitoring
- Vulnerability scan run

Vulnerability risks
Vulnerability assessment scans are run periodically to identify security issues. You can trigger a vulnerability scan from IBM Data Risk Manager or import from various sources to identify vulnerabilities. Vulnerability risks are evaluated based on combined weightage of the following risk factors.

- Severity and count of the vulnerabilities that are discovered.
- Status of the remediation actions.

Monitoring risks
Threats are logged to the syslog server (alert events) from various integration servers that are configured with IBM Data Risk Manager. Monitoring risks are evaluated based on combined weightage of the following risk factors.

- Severity and count of the alerts that are logged.
- Status of the remediation actions.

Qualitative risks
Qualitative risk analysis evaluates and documents the probability and the impact of assessment risks against a pre-defined scale. IBM Data Risk Manager assessment risks are evaluated based on combined weightage of the following risk factors.

- Severity and count of the risks.
- Status of the remediation actions.
- Status of the risks.

Participation

The participation of an infrastructure node to an information asset determines contribution of the node towards the risk score. The participation is determined as a percentage of data elements, which is contributed by the node towards the information asset.

Visualizing risks by using IBM Data Risk Manager

IBM Data Risk Manager provides comprehensive and dynamic views of data-related business risks to business leaders. An intuitive business risk dashboard and control center help to uncover, analyze, and view risks for taking right actions to protect the business.

IBM Data Risk Manager provides multi-level visibility into information asset risks through the following two views:

- Information Asset Portfolio
- Privacy Splash

Information Asset Portfolio

The information asset portfolio is the result of discovery and classification of data, and is a logical grouping of data assets according to a taxonomy. The taxonomy is configurable and is associated with the business context of the organization. Run the following steps to view the **Information Asset Portfolio** page.

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) with your user credentials.
2. Click the menu icon ⠿.
3. Click **Dashboard**.
4. Select your program.
5. Click **Dashboard**. The **Information Asset Portfolio** page displayed.

An information asset can be `High`, `Medium`, or `Low` priority, based on the pre-defined scoring criteria.

For more information about information asset portfolio, see "IBM Data Risk Manager Dashboard" on page 164.

Privacy Splash

Privacy Splash page is the landing page of IBM Data Risk Manager Dashboard module. The **Privacy Splash** page provides a broader overview of the privacy data risk exposure of information assets through a series of charts, maps, graphs, tables, and more. You can visualize and manage information in various widgets in different ways that helps business leaders to quickly analyze and address data privacy risks to protect their organizations.

Run the following steps to view the **Privacy Splash** page widgets for a specific program.

1. Click **Program** to select your program from the list.
2. Click **Privacy Splash**.
3. Click the Reload Widget icon ↻ on each of the widgets to refresh data.

For more information about **Privacy Splash** widgets, see "IBM Data Risk Manager Privacy Splash" on page 160.

Configuring color schemes for widget visualizations

You can customize default colors of various IBM Data Risk Manager widget elements with user-configured colors according to your requirements.

About this task

The colors can be customized for the following items.

- Splash Widgets
- Widgets in Security Command and Control
- IBM Data Risk Manager Dashboard

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**.
4. Click the drop-down icon ⌄ and select **Widget Configuration**.
5. Click the drop-down icon ⌄ next to a widget title, for example, **Splash Widgets**.
6. To modify default color scheme for the **Geographic Distribution of Information Assets with country specific drill down** widget elements, run the following steps.
   a) Select **Data Residency**.
   b) Click the edit icon ✎.
   c) In the color palette, select a color as per the requirements.
   d) Click **OK**.
   e) To restore default color of the widget, click the restore icon ↻.
   f) To modify color for other items under **Geographic Distribution of Information Assets with country specific drill down**, click the drop-down icon ⌄ and select an item from the list, for example **Policy Violations**.
   g) Repeat the Steps b - d.
   h) Repeat the same steps to modify color schemes for the items under **Policy Violations and Vulnerabilities pertaining to the Information Asset**.
7. Repeat the same steps to modify color schemes for the items under **Security Command and Control Center** and **IBM Data Risk Manager Dashboard**.

IBM Data Risk Manager Privacy Splash

You can visualize data security and privacy information in various IBM Data Risk Manager Privacy Splash widgets in different ways that helps business leaders to quickly analyze and address security and privacy risks to protect their organizations.

Privacy Splash page is the landing page of IBM Data Risk Manager Dashboard module. The **Privacy Splash** page provides a broader overview of the security and privacy risk exposure of information assets through a series of charts, maps, graphs, tables, and more.

To view the **Splash** page widgets for a specific program:

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`) with your user credentials.

2. Click the menu icon ⠿.
3. Click **Dashboard**.
4. Click **Program** to select your program from the list.
5. Click **Privacy Splash**.

The following widgets are included in IBM Data Risk Manager Privacy Splash page.

- Geographic Distribution of Information Assets
- Information Asset Distribution
- Top 10 Data Flows
- Policy Violations and Vulnerabilities
- Classification
- Quarterly Vulnerabilities Trends

Run the following steps to display widgets that you need on the **Privacy Splash** page.

1. Click the **Widgets** icon 6 Widgets ⌄ for selecting widgets to view on the page.
2. Select the widgets that you want to display on the **Privacy Splash** page.
3. Click **Apply** to save your settings.

To refresh data on the widgets, click the Reload Widget icon ⟳ on each of the widgets.

Geographic Distribution of Information Assets

The Geographic Distribution of Information Assets widget on the IBM Data Risk Manager **Privacy Splash** page shows data locations, policy violations, vulnerabilities, and application locations that are associated with an infrastructure on a global map.

The **Data Sources + Residency** section shows summary information that includes total number of data source locations, data sources, table row counts and columns, and the risks that are associated with the infrastructure. The **Applications + Business Processes** section shows summary information that includes total number of applications, business processes, data flows, and data risks that are associated with the application inventory.

Data Residency

Enable the **Data Residency** toggle button to view distribution of sensitive data residency across countries. Move cursor on highlighted circles on the global map to view data residency information across countries. On left side of the widget, country names are displayed along with the data element numbers.

Select a country from the list and click the arrow icon → to view state-wise distribution of data on the map. This icon for drill-down view is displayed only for the supported countries. Click the details icon ••• to view list of states and the associated data. To deselect your country selection, click the country name again or click the **Reload Widget** icon ⟳.

Policy Violation

Enable the **Policy Violation** toggle button to view the policy violations that are associated with the infrastructure. Move cursor on highlighted circles on the global map to view policy violation details across countries. On left side of the widget, country names are displayed along with the policy violation numbers.

Select a country from the list and click the arrow icon → to view state-wise distribution of data on the map. This icon for drill-down view is displayed only for the supported countries. Click the details icon ••• to view the list of states and the associated data. To deselect your country selection, click the country name again or click the **Reload Widget** icon ⟳.

Vulnerabilities

Enable the **Vulnerabilities** toggle button to view vulnerability information that is associated with the databases, endpoints, and application inventories. Move cursor on highlighted circles on the global map to view vulnerability information across countries. On left side of the widget, country names are displayed along with the vulnerability numbers.

Select a country from the list and click the arrow icon to view state-wise distribution of data on the map. This icon for drill-down view is displayed only for the supported countries. Click the details icon to view the list of states and the associated data. To deselect your country selection, click the country name again or click the **Reload Widget** icon.

Application Residency

Enable the **Application Residency** toggle button to view location of applications across geographies. On left side of the widget, name of the applications are displayed.

When an application is selected from the left pane, global presence of that particular application is plotted on the global map. You can view following details for the selected application.

- Application server icon shows the application server count.
- Database server icon shows the database server count.
- Click the details icon to view mapping information of application server and database server and their count. Meaning of `Unmapped` is that the server location is not known. You can view the mapped server locations on the map.
- To deselect your application selection, click the application name again or click the **Reload Widget** icon.
- To deselect a country selection on the map, click the cross icon next to the country name in the left pane.

Supported countries are Germany, United States of America, Canada, Australia, Russia, UAE, UK, India, Afghanistan, France, South Africa, Italy, Netherlands, Brazil, Japan, China, Spain, Argentina, Mexico, Colombia, Chile, Paraguay, Bolivia, Uruguay, Venezuela, Mongolia, North Korea, South Korea, Singapore, New Zealand, Saudi Arabia, Yemen, Oman, Romania, Bulgaria, Greece, Turkey, Portugal, Israel, Switzerland, Austria, Belgium, Poland, Sweden, Norway, Finland, Ukraine, Belarus, Ireland, Denmark, Czech, Slovakia, Hungary, Croatia, and Serbia.

Use following icons on the widget to change map size and to refresh data.

- Click the reset icon to reset map size.
- Click the zoom in icon and zoom out icon to change map size.
- Click the **Reload Widget** icon to refresh data.

Information Asset Distribution

The Information Asset Distribution widget on the IBM Data Risk Manager **Privacy Splash** page shows privacy risk and the security risk details of information assets that are associated with the selected program.

To display the risk information, you can select taxonomy-related attributes to indicate whether the information asset has crown jewel information, non-crown jewel information, or both. Listed entities are the typical taxonomy-mapping attributes in context data such as Application, Group Organization level, Consuming Organization level 1, Consuming Organization level 2, Business process, and Assets.

All the assets that are associated with the program are listed. Sort order is determined by classification, crown jewel, critical category, and sensitivity level. The asset risks are displayed for the respective assets.

Only the top 10 applications, business processes, and other taxonomy attributes are displayed. Associated application level data risks and privacy risks are also displayed.

Privacy Risk

You can view asset inventories and their corresponding privacy risk information in tabular format. The chart shows privacy risk distributions for the associated inventories (application or database).

Taxonomy

Asset risk details are shown in tabular format for the selected entities. Click the **Configure** icon ⚙ to select the entities. You can filter data display by selecting the necessary data classification categories. The chart shows risk distributions across infrastructures.

To refresh data, click the **Reload Widget** icon ↻ on the widget.

Top 10 Data Flows

The Top 10 Data Flows widget on the IBM Data Risk Manager **Privacy Splash** page shows the data flow maps to quickly visualize where the sensitive data is processed, how it transits, and where it is stored. The flow diagrams show the relationships among business entities of an organization, for example, business processes, applications, and infrastructure.

You can view the data flow diagrams based on data sources, business processes, and applications. To view more details, move the cursor on a diagram element.

Data Source

Data flow diagram is displayed for the selected data source to view data risk and privacy risk information.

Application

Data flow diagram is displayed for the selected application to view data risk and privacy risk information.

Process

Data flow diagram is displayed for the selected process to view data risk and privacy risk information.

To refresh data, click the **Reload Widget** icon ↻ on the widget.

Policy Violations and Vulnerabilities

The Policy Violations and Vulnerabilities widget on the IBM Data Risk Manager **Privacy Splash** page shows the breakdown of policy violations and vulnerabilities across information assets.

The chart shows the top 10 information assets. You can also view the icons that indicate risk level and crown jewel details of the information assets. Sort order is determined by classification, crown jewel, critical category, and sensitivity level.

To refresh data, click the **Reload Widget** icon ↻ on the widget.

Classification

The Classification widget on the IBM Data Risk Manager **Privacy Splash** page provides you with a quick view about security classification of information assets. Data classification details are presented in the form of pie chart and list view format that helps communicate information clearly and effectively.

To view the classification information in the form of a pie chart, click the pie chart icon ◕. Chart view is the default view.

To view the classification information in the list view format, click the list view icon ☰.

You can view the data classification information based on the following criteria. Select the options **All**, **With Crown Jewel**, or **Without Crown Jewel** to display the classification information to meet your needs.

Categories

Click **Categories** to view the data classification information based on various categories. Hover on slices of the pie chart to view the percentage value for different categories. Click on a slice to display the detailed information.

Tagged Assets

Click **Tagged Assets** to view the data classification information based on a tag name that identifies a group of related information assets. Hover on slices of the pie chart to view the percentage value for different tagged assets. Click on a slice to view the detailed information.

Compliance

Click **Compliance** to view the data classification information based on regulatory obligations that are associated with the asset such as HIPAA, SOX, or PCI. Hover on slices of the pie chart to view the percentage value for different compliance information. Click on a slice to view the detailed information.

To refresh data, click the **Reload Widget** icon ↻ on the widget.

Quarterly Vulnerabilities Trends

The Quarterly Vulnerabilities Trends widget on the IBM Data Risk Manager **Privacy Splash** page shows details of quarterly vulnerability trends for the scans that are run across various databases endpoints and application platforms. Move the toggle button to view trends of passed and failed vulnerability scans.

Platforms that are associated with the information assets are displayed below the chart. Click a platform to view detailed information pertaining to the vulnerabilities based on the severity details such as Critical, Major, Minor, or Caution.

To refresh data, click the **Reload Widget** icon ↻ on the widget.

IBM Data Risk Manager Dashboard

IBM Data Risk Manager Dashboard is an interactive dashboard that enables information governance by providing visualization and management in a single unifying console that depicts potential risks to sensitive business assets.

IBM Data Risk Manager Dashboard functions

- Provides an interactive visualization of the information assets portfolio, data classification, and security requirements.
- Enables the application of proactive security controls and risk mitigation by providing visibility to potential risks, exposures, and vulnerabilities.
- Combines information assets, processes, and controls metadata to represent the data security and governance posture.
- Enables information governance by helping business leaders to visualize risks to sensitive assets across business functions and to understand potential organizational impacts.
- Provides compliance oversight through real-time notifications and action items in alignment with data security policies and requirements.

Information Asset Portfolio

The **Information Asset Portfolio** widget on the dashboard shows classification of all the information assets that are associated with a program based on a user-selected taxonomy model. Information asset is the central concept of IBM Data Risk Manager and can be defined as an aggregation or grouping of related data elements that together represent a business asset.

The asset portfolio provides the following functions.

- Display all information assets that are associated with a program.
- Visualize the information assets in a manner that represents business sense.

Default view shows information assets that are associated with the selected program. The X-axis shows information classifications. Y-axis shows program and subprograms. You can dynamically modify the taxonomy representation. This taxonomy is configurable to the business context of the organization. To change the X and Y axes attributes for a program, run the following steps.

1. Click the program on X-axis.
2. Click the arrow buttons ▶ ▼ next to the labels to select your attributes.

When you select an information asset on the **Information Asset Portfolio** widget, all metadata that are associated with the selected information asset is displayed in the surrounding widgets such as **Infrastructures**, **Stakeholders**, **Processes**, and **Applications**.

The various micro-icons and numbers on an information asset provides the following business and technical metadata details that are associated with the selected information asset.

Icon	Description
⚠ 26	Numeric next to the icon indicates number of policy violations. Click the icon to view incidents on Asset Logs window that are logged (by severity) against the selected information asset. On the **Asset Logs** window, click the items to view the alert details.
☰ 24	Numeric next to the icon represents number of granular data elements that are associated with the information asset.
✣	Click the icon to view Confidentiality-Integrity-Availability (CIA) rating for the information asset.
♔	Indicates that the information asset has crown jewel information.
● ● ● ●	Represents the risk score for the information asset such as high (red), medium (amber), low (green), or no risk (gray). Click the icon to view the factors that are considered to calculate risk score.

You can customize default colors of the information asset card and the associated metadata elements. For the steps on how to customize colors, see "Configuring color schemes for widget visualizations" on page 160.

Use following icons on the **Information Asset Portfolio** widget to run various tasks.

- Enable the **Display All Level Data** toggle button to view assets of the child level programs too for a selected parent program.
- Enable the **Show Asset Tags** toggle button to view information for the assigned tags. Click the **Filter Assets Based on Tag** icon 🏷 to display assets based on the selected tag.
- Click the **Filter Assets** icon ▽ to view information assets based on attributes such as `Crown Jewels`, `Information Classification`, or `Compliance`.
- Click the refresh icon ⟳ to refresh widget data.
- Click the expand icon ↗ to expand the widget area.
- Click the arrow icon → on the information asset to view more details of data elements on the **Asset Details** window.

Information asset drill-down

On the **Information Asset Portfolio** widget, click the arrow icon → on the information asset to display the **Asset Details** popover for viewing details of the selected asset.

Overview

Provides granular information about the tables and columns where the information asset resides and list of assigned attributes for the associated applications.

Note: Unstructured assets are not associated with any applications. Therefore, taxonomy attributes are not applicable for unstructured assets.

Infrastructure

You can view the following information.

- List of data sources with details such as data contribution percentage, IP address, port number, data source location, and stakeholders.
- Policy violations that are logged against the infrastructure nodes under **Policy Violations**.
- Vulnerabilities that are logged against the infrastructure nodes under **Vulnerabilities**.
- Risks that are that are associated with the infrastructure nodes under **Risks**.

You can view the policy violations, vulnerability details, and risk information based on the selected filter option such as sources or severity. When you select a policy violation, vulnerability, or risk item, you can view the following information.

- More details about the selected item under **Details**.
- Remediation actions that are defined for the selected item under **Action Items**.
- Mail configuration under **Mail**.

Infrastructures

The Infrastructures widget shows infrastructures (platforms) that are associated with the information asset. Data elements can include both structured and unstructured repositories. Click the drop-down icon ⌄ on an infrastructure to view data repositories and their attributes. Following attributes are shown for the selected repository.

- Data repository name, IP address, port, and geographical location.
- Number of alerts that are logged against the infrastructure node.
- Number of vulnerabilities that are logged against the infrastructure node.
- Data contribution percentage.
- Encryption status icon indicates whether the data source is encrypted.
- Monitoring status icon indicates whether the data source is monitored.
- Vulnerability scan status icon indicates whether the vulnerability assessment scan is run on the data source.
- Data Risks icon indicates whether the risk score is high (red), medium (amber), or low (green) for this specific infrastructure. Click the icon to view details of various risk vectors along with the associated factors that are considered for risk calculation. You can also view impact level that is calculated based on the taxonomy attributes of information asset and the risk score of infrastructure.
- Privacy Risks icon indicates whether the privacy risk score is high (red), medium (amber), or low (green) for this specific infrastructure.
- Click the maps icon to view relationship of this infrastructure with other entities such as business processes and applications that are associated with the information asset.

- Click the download icon ⤓ to download the CSV files that contain infrastructure-specific attributes.
- Click the data maps icon ⇥ to view pop-over, which displays infrastructure-specific attributes that are configured and grouped based on a context.

Stakeholders

The `Stakeholder` widget shows the stakeholders who are associated with the selected information asset. The widget can be configured to represent a stakeholder framework that can be customized to an organization. Click on any of the slices of the pie to view the corresponding stakeholder in the organization.

Processes

The `Processes` widget shows the business processes that are associated with the selected information asset. These are the business processes in an organization that are depend on the information asset to perform business transactions. Attributes that are associated with business processes can be customized to the organization structure.

On a selected process, click the ••• icon to view pop-over, which displays business process-specific attributes that are configured and grouped based on a context. To download the PDF file with process-specific attributes, click the download icon ⤓.

Applications

Application widget shows applications that are associated with the selected information asset. These are the applications that produce, consume, or use the information asset. Attributes that are associated with applications can be customized to the organization structure. Vulnerability and alert counts are shown if the hosted application server contains associated vulnerabilities and policy violations. Following attributes are shown for the selected application.

- Number of alerts that are logged against the hosted application server. Click the number to view more details.
- Number of application vulnerabilities that are logged against the hosted application server.
- Data Risks icon indicates whether the data risk score is high, medium, or low for this specific application server.
- Privacy Risks icon indicates whether the privacy risk score is high, medium, or low for this specific application server.
- Click the data maps icon → to view pop-over, which displays application-specific attributes that are configured and grouped based on a context.
- Click the download icon ⤓ to download the PDF file with application-specific attributes.

Risks, Exposures, and Vulnerabilities (REV) Reporting

IBM Data Risk Manager can be used to identify potential risks to sensitive business information assets. Based on the availability of such information, IBM Data Risk Manager overlays risk vectors that are composed of activity monitoring incidents, exposures and vulnerabilities, and potential malicious activity at multiple levels. Risk vectors provide visibility into appropriate stakeholders and enable them to initiate remedial measures. For example, risk vectors that are overlaid over information assets provide a business stakeholder warning on a risk that is associated with the business asset, while such information overlaid over data repositories is indicative to a technical stakeholder.

Framework Builder

You can use the IBM Data Risk Manager Framework Builder component to create and manage frameworks, questionnaire templates, questionnaires, and registers that are necessary to perform assessments.

IBM Data Risk Manager Framework Builder provides the following functions.

Framework Builder
To create and manage assessment frameworks, topics, subtopics, and factors. For more information about Framework Builder, see "IBM Data Risk Manager Framework Builder" on page 168.

Questionnaire Builder
To create and manage questionnaire templates and questionnaires. For more information about Questionnaire Builder, see "Questionnaire Builder" on page 170.

Register Definitions
To manage registers and create register items. For more information about Register Definitions, see "Register Definitions" on page 174.

IBM Data Risk Manager Framework Builder

You can use IBM Data Risk Manager Framework Builder component to create and manage frameworks that are necessary to perform risk assessments. A framework is a regulatory or compliance requirements against which an organization's control implementations are measured for data compliance.

An assessment framework consists of the following objects.

Topic
The first level of a framework hierarchy with one or more subsections, each of them addressing a control object. A topic is an aggregation of subtopics.

Subtopic
Includes generic functional requirement specifications for a framework with associated controls. A subtopic is an aggregation of factors.

Factor
The lowest level of a framework hierarchy with associated controls.

Assessment frameworks

You can create the following types of assessment frameworks by using IBM Data Risk Manager Framework Builder.

PRA
Creates framework to assess controls in alignment with General Data Protection Regulation (GDPR) regulatory requirements. When you create an assessment, if you select GDPR framework, five assessments are created by default.

Non-PRA
Creates framework to assess controls in alignment with non-GDPR regulatory requirements, for example, ISO framework. To create an assessment, you must use topics, subtopics, and factors that are created by using Framework Builder.

Creating a framework

You can use IBM Data Risk Manager Framework Builder to create and manage frameworks that are necessary to perform data risk assessments.

About this task

An assessment framework consists of the following objects.

Topic
The first level of a framework hierarchy with one or more subsections, each of them addressing a control object. A topic is an aggregation of subtopics.

Subtopic
Includes generic functional requirement specifications for a framework with associated controls. A subtopic is an aggregation of factors.

Factor
The lowest level of a framework hierarchy with a set of questions about a control implementation.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Framework Builder** > **Framework Builder**.
4. On the **Framework Builder** section, set the following options, and click **Create**.

Option	Description
Name	Name of the framework.
Display Name	Display name for the framework.
Description	Description of the framework.
Controls	Selection of data security controls to associate with the framework. You can define more controls in **Register Definitions** for a predefined register, for example, `DictControl`.
Assign	Selection of a questionnaire template to associate with the framework. The templates that are created in **Questionnaire Builder** are listed in the **Assign** list.
Framework Type	Selection of assessment framework type, for example, **NON PRA** or **PRA**. Select PRA to create GDPR framework. Select `NON` PRA to create non-GDPR framework.

What to do next

Create topics, subtopics, and factors for the framework that you created. For more information, see "Creating a topic, subtopic, and factor for a framework" on page 169

Creating a topic, subtopic, and factor for a framework

Associate a topic, subtopic, and factor for the assessment framework that you created. A framework is a regulatory or compliance requirements against which an organization's control implementations are measured for data compliance.

Before you begin

Ensure that the frameworks are created and available for use.

About this task

An assessment framework consists of the following objects.

Topic
The first level of a framework hierarchy with or more subsections, each of them addressing a control object. A topic is an aggregation of subtopics.

Subtopic
Includes generic functional requirement specifications for a framework with associated controls. A subtopic is an aggregation of factors.

Factor

The lowest level of a framework hierarchy with a set of questions about a control implementation.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⋮⋮⋮.
3. Go to **Business Context Modeler** > **Framework Builder** > **Framework Builder**.
4. Under **Created Framework**, click **Topics** on the framework for which you want to create a topic.
5. On the **Framework Builder** section, set the following options.

Option	Description
Name	Name of the topic.
Display Name	Display name for the topic.
Description	Description of the topic.
Controls	Selection of data security controls to associate with the topic. You can define more controls in **Register Definitions** for a predefined register, for example, `DictControl`.

6. Click **Create**.
7. Create a subtopic.
   a) Under **Created Topics**, click **Sub Topics** on the topic for which you want to create a subtopic.
   b) Specify necessary details in the respective fields that meet your business needs.
   c) Click **Create**.
8. Create a factor.
   a) Under **Created Sub Topics**, click **Factors** on the subtopic for which you want to create a factor.
   b) Specify necessary details in the respective fields that meet your business needs.
   c) Click **Create**.

Questionnaire Builder

Use IBM Data Risk Manager Questionnaire Builder function to create and manage templates and questionnaires that are necessary to perform assessments.

Questionnaires

Questionnaires are created for gathering user responses to assess readiness or understand maturity of controls. Use the IBM Data Risk Manager assessment questionnaires to define and associate context flows required for evidence collection and delegation, and to capture context attributes such as priority, significance, relevance, and applicability. Questions can be associated with multiple templates and customized to use across multiple assessment frameworks. Depending on the type of responses expected for a question, appropriate question type is created and configured. For the steps on how to create questionnaire, see "Creating a question" on page 172.

Importing questionnaire data

You can also import a predefined questionnaire for use in the assessment. Data is defined for assessment questionnaire, response type, and registry in a comma-separated value (CSV) file, which you can import into IBM Data Risk Manager. For more information about how to import questionnaire data, see "Importing assessment questionnaire, response type, and registry as CSV file" on page 175.

Questionnaire templates

A questionnaire template is an assessment instrument that is composed of a series of questions and other instructions for gathering responses from individuals to evaluate maturity of a control. You can reuse the templates across multiple assessment frameworks. For the steps on how to create a questionnaire template, see "Creating a questionnaire template" on page 171.

Decision tree

Responses to some questions lead to further questions. You can express this relationship by creating a conditional relationship between questions. In a conditional relationship, there is a parent question and a child question. The child question is, by default, not displayed. The child question is displayed only when an enabling response is provided to the parent question. By using the decision tree, you can quickly view and identify the relationships between the questions.

Decision tree is a hierarchical structure that consists nodes and directed edges. A decision tree typically starts with a single node (parent question), which branches (child questions) into possible outcomes. Each of those outcomes can lead to additional nodes, which branch off into other possibilities. By using a decision tree, you can easily explain the decisions, identify possible events that might occur, and see potential outcomes.

Creating a questionnaire template

You can use IBM Data Risk Manager Questionnaire Builder to create a questionnaire template. A template can be associated with series of questions and other instructions that are intended for gathering responses from individuals. You can reuse a template across multiple assessment frameworks.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Framework Builder** > **Questionnaire Builder**.
4. To create a template click **New Template**.
5. On the **Create Template** section, set the following options, and click **Create**.

Option	Description
Name	Name of the template.
Category	Template category, for example, `Assessment`.
Description	Template description.
Scoring Model	Scoring model to be used for assessment score calculation, for example, `Weighted Average` or `Conditional Method`.
Calculation Methodology	You can specify a score calculation method only when you select `Conditional Method` from the **Scoring Model** list.
Scorecard Template	You can specify a scorecard template with predefined scoring scale. If you select `Conditional Method` from the **Scoring Model** list, you can set conditions for the selected scorecard template.

Creating a question

You can use IBM Data Risk Manager Questionnaire Builder to create questions for the assessment and associate them with multiple questionnaire templates.

About this task

You can also define data for assessment questionnaire in a comma-separated value (CSV) file, which you can import into IBM Data Risk Manager. For the steps on how to import questions, see "Importing assessment questionnaire, response type, and registry as CSV file" on page 175.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Framework Builder** > **Questionnaire Builder**.
4. To create a question click **New Question**.
5. On the **Create Question** section, set the following options, and click **Save**.

Option	Description
Questions	Text for of the question.
Description	Description for the question.
Question Priority	You can prioritize question for the defined framework by specifying the high, medium, info, or low priority. You can add an item to the **Question Priority** list by creating a register item for the **Question Priority** register in **Business Context Modeler** > **Framework Builder** > **Register Definitions**. For the steps about how to create a register item, see "Creating an item and subitem for the register" on page 174.
Question Group	You can associate the question with a predefined group. During assessment, you can view the questions with responses based on the group that you assigned when the question is created. You can add a group to the **Question Group** list by creating a register item for the **Question Grouper** register in **Business Context Modeler** > **Framework Builder** > **Register Definitions**. For the steps about how to create a register item, see "Creating an item and subitem for the register" on page 174.
Answer Type	Display type for the answer options, such as multiple selection list, radio button, and scale type.
Chapter	Chapter number of the framework.
Section	Section number of the framework.
Article	Article number of the framework.
Reference Article	Reference article number of the framework.
Question Dependency	Responses to some questions lead to further questions. You can express this relationship by creating a conditional relationship between questions and showing them in the form of a decision tree. a. Click the add icon ➕. b. Select **And** or **OR** according to the requirements.

Option	Description
	c. Select dependent questions from the list. d. Set the conditions for attributes of the selected questions. e. Click **Save Conditions**.
Answer Options	Define the answer options for the question. a. Click the add icon ➕. b. Specify the answer text in **Answer Text**. c. Add description about the answer in **Description**. d. Assign a score value. 1) Specify an answer score in the range 0 - 5 in **Answer Score**. To provide answer to **Scale** type question, specify values in **Minimum Value**, **Maximum Value**, and **Scale Value Descriptions** fields. 2) Select the context type from **Context Type**. 3) Click **Add** to define observations by specifying a priority. Specifying answer score is not needed when the computational score is generated by selecting **Computational Scoring**. e. For generating computational score, run the following steps. 1) Select **Computational Scoring**. 2) Select **Standard** to assign score based on the other answers that you select. 3) Select an option from the **Computation Formula** list. 4) Select the answers from the **Answer to be considered** list. 5) Select **Conditional** to assign score based on the conditions that you define. 6) Click the add icon ⊕ to add a condition. 7) Specify values in the **Method**,**Operator**, **Value**, and **Score Value** fields. f. If you want the answer score to be considered for the assessment, select **Consider For Scoring**. g. Specify the answer keywords in **Answer Keywords**. h. Click **Save Answer**.
Register	Register that is associated with the question.
Scope	Items are displayed for your selection based on the register that is selected in **Register**.

6. The question that you created is listed on the **All Questions** section. You can associate templates to the question that you created.

   a) Select the questions from the list.

   b) Click **Assign**.

   c) Select templates from the **Assign Templates** list.

   d) Click **Confirm**.

   e) To modify the template selection information, click **Template**.

7. Click **Decision Tree** on a question to view the conditional relationship between questions in decision tree format.
8. The **Dependent Question** icon on a question represents conditional relationship with other questions.
9. Click **Filter** to display questions that are associated with the **Register** and **Scope** that you select.

Register Definitions

You can use IBM Data Risk Manager Register Definitions to create items and subitems for the predefined registers. These items and subitems are used for assessment framework creation.

Creating an item and subitem for the register

You can use IBM Data Risk Manager Register Definitions to create items and subitems for a predefined register.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Go to **Business Context Modeler** > **Framework Builder** > **Register Definitions**.
4. Select a register from the **Registers** list.
5. To create an item click **New Register Item**.
6. Set the following options, and click **Save**.

Option	**Description**
Name	Name of the item.
Display Name	Display name of the item.
Description	Description for the item.

   The item that you crated is displayed in the **Items** list.
7. To add a subitem, select an item from the list.
   a) Click the **Add**.
   b) Specify the information for subitem such as name, display name, and description.
   c) Click **Save**.
8. To add a property to the item, run the following steps.
   a) Click **Property**.
   b) Click the add icon ⊕.
   c) Specify the name in **Property Name**.
   d) Specify the value in **Property Value**.
   e) Click **Save**.
   f) Click the **Property Value** color box icon to choose property color to display on IBM Data Risk Manager Dashboard.
9. To assign items for a selected item, run the following steps.
   a) Click the **Assign** icon ⊕.
   b) Select items from the list.
   c) Click **Assign**.

Importing assessment questionnaire, response type, and registry as CSV file

You can define data for assessment questionnaire, response type, and registry in a comma-separated value (CSV) file, which you can import into IBM Data Risk Manager.

Before you begin

Ensure that the business context data is available for importing.

You can download the sample templates at: http://www.ibm.com/support/docview.wss?uid=ibm10731739

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⋮⋮⋮.
3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**.
4. Enable the **Catalog Data** toggle button.
5. Click the **Assessment** tab.
6. Load the CSV file for response type.
   a) Under **Response Type**, click **Browse** to locate and select the file.
   b) Click **Load**.
   Data is displayed for your verification.
7. Load the CSV file for assessment questionnaire.
   a) Under **Questionnaire**, click **Browse** to locate and select the file.
   b) Click **Load**.
   Data is displayed for your verification.
8. Load the CSV file for registers.
   a) Under **Registry**, click **Browse** to locate and select the file.
   b) Click **Load**.
   Data is displayed for your verification.
9. Click **Import**.

Assessments

You can use the Assessment component of IBM Data Risk Manager to create assessments. An assessment is a custom or industry-standard set of questions that produces a result. Assessments are a means of gathering information from business users in the organization. Assessment results can then be used to determine asset valuations, gap analysis, risk score, and for remediation planning.

The IBM Data Risk Manager Assessment feature provides a data security framework to assess controls in alignment with regulatory requirements. The assessment is driven by using questionnaires and a consolidated scorecard.

- Platform to create custom assessment for the selected data security, governance, and management regulations and frameworks such as ISO 27002.
- You can assess and understand readiness for compliance regulations such as General Data Protection Regulation (GDPR), corporate policies, procedures, and guidelines.
- Capture or source information with custom templates to gather responses, evidences, notes, and reassignments.

- Capture context data entities information during assessment evaluation for risk score calculation.
- Interactive scorecard and reports for both readiness and maturity assessments.
- Integration with IBM Data Risk Manager Action Center to create and manage remediation action items for addressing gaps in the assessment.

The **Business Context Modeler** > **Framework Builder** component of IBM Data Risk Manager is used to create the assessment structure and workflow definition such as framework modeling and questionnaire development. For more information about Framework Builder, see "Framework Builder" on page 168.

Assessment scoping

During assessment program creation for non-PRA-based frameworks, you can define scope of the assessment in terms of business entities or domains such as business processes, applications, and assets. Assessment scoping ensures that the necessary data is collected in effective and efficient manner for risk evaluation.

Risk modeling

Risk is calculated based on various factors such as significance of a specific question, associated response, assigned assets and their importance (ranking), mapped threats and events, and other such criteria that are defined as part of customization of the questionnaire.

The responses to the assessment questionnaire are factored into determining the overall risk score and remediation actions. These criteria might include sensitivity factors such as Confidentiality, Availability and Integrity (CAI), and business impact such as associated cost, asset ranking, or importance. Residual risk is automatically calculated and the score is adjusted based on the completion of action items that are defined to address gaps or findings, if any.

Assessment for GDPR

IBM Data Risk Manager is enabled with General Data Protection Regulation (GDPR) that is adopted by the EU and EEA countries. It establishes harmonized and strengthened protection for personal data of individuals. IBM Data Risk Manager supports data compliance by providing assessment and questionnaire. With IBM Data Risk Manager assessment implementation, the following requirements are handled.

- Visibility into security risk posture that is associated with sensitive data.
- Wider definition of personal data, including location information and online identifiers.
- New obligations for processors with contractual, operational, and technical impact.
- Helps to enable security by analyzing various gaps in the current data security environment.
- Helps to determine the controls and prioritize the tasks to remediate gaps, and to develop an action plan.

Assessment Outcome Management

Based on non-PRA assessment results, appropriate actions need to be implemented for addressing and mitigating the identified risks. You can use the Assessment Outcome Management module of IBM Data Risk Manager to view and manage risks. For more information about outcome management, see "Assessment Outcome Management" on page 186.

User persona for assessments

Assessment User Persona	Capabilities	Description

Administrator	Program definition and management	Establish scope and boundaries for assessment as a program that is based on various factors such as business units, platforms, users, and roles.
	Framework building and configuration	Define and develop custom frameworks for assessments with various categories and associate questions for the various factors, tags, and templates.
	Assessment modeling • Questions definitions • Templates creation • Assessment programs definitions	Define questions, answer options for the associated responses, add to templates, and assign to framework topics, subtopics, and factors.
	User and access provisioning	Define users and roles for various resources to access IBM Data Risk Manager, and provide access to programs and assessments.
Assessor **C3 Assessment User** (IBM Data Risk Manager user role)	Assessment definitions and interview creation	Define assessments based on framework and create interviews for the respective assessments to calculate the risk scores based on gap analysis and findings.
	Information capture and risk scoring	Responses to questionnaire are captured through available options that are set in the response template. Pre-defined responses, significance of associated questions, notes, and descriptions are captured.
Reviewer **C3 Assessment User** (IBM Data Risk Manager user role)	Review and sign off assessment	View responses such as answers, notes, and evidences that are provided by the Assessors to assessment questions, perform validation, and sign off on the assessment reports.

Creating an assessment program

Use the Assessment component of IBM Data Risk Manager to create an assessment program for the assessment.

Before you begin

Ensure that necessary assessment frameworks are created in Framework Builder to meet your requirements. For more information about Framework Builder, see "Framework Builder" on page 168.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Click **Assessment**.
4. On the **Assessment** page, select a program from Program list. Scope and boundaries for the assessment is established as a program that is based on various factors such as business units, platforms, users, and roles.
5. In the **Assessment Program List** section, click the **Create Assessment Program** icon ⊕.

6. On the **Create Assessment Program** page, set the following options, and click **Create Assessment Program**.

Option	Description
Can be Shared	Select to share or reuse the responses of this assessment program with other assessments.
Name	Name of the assessment.
Framework	Framework to be used for the assessment. The frameworks that are crated in Framework Builder are available for the selection.
Entity	List of entities or domain names for Non-PRA-based assessments. Select business entities or domain names to define scope of the non-PRA-based assessments. Assessment scoping ensures that the necessary data is collected in effective and efficient manner for risk evaluation.
Start Date, Duration, Unit	**Start Date** Assessment start date. **Duration** Assessment duration. **Unit** Unit of measure, for example, `Day`, `Week`, or `Month`.
Description	Description of the assessment.
Objectives	Purpose and goal of the assessment.
Department	Department name of your organization where the assessment program is being performed.
Line of Business	Line of business that is associated with the assessment.
Security Classification	Security classification of the information asset.
Global Risk ID	Global risk identification number that is mapped to relevant service offerings.

What to do next

Create an assessment. For the steps on how to create an assessment, see "Creating an assessment for GDPR framework" on page 178 and "Creating an assessment for non-GDPR framework" on page 179.

Creating an assessment for GDPR framework

For creating your assessment, you can use the five assessments that are generated for GDPR framework (PRA framework).

Procedure

1. Create an assessment program by selecting GDPR framework (PRA framework) to create the assessment. For the steps on how to create an assessment program, see "Creating an assessment program" on page 177.
2. When an assessment program is created with GDPR framework, by default, five GDPR assessments are displayed on the **Create Assessment** page to create your assessment for GDPR framework.

   You can exclude a default assessment from the list when you create the assessment. To exclude, select an assessment and click the exclude icon .
3. Click **Create Assessment**.

What to do next

Assign resources to the assessment that you created. For the steps on how to assign resources, see "Assigning resources to run assessment" on page 179.

Creating an assessment for non-GDPR framework

Use the Assessment component of IBM Data Risk Manager to create an assessment by using a non-GDPR framework (non-PRA framework), for example, framework for ISO 27002.

About this task

Based on the framework selection during assessment program creation, associated topics, subtopics, and factors are populated. Each of the selected topics forms an assessment. For more information about creating a framework, see "Framework Builder" on page 168.

Entities with their concepts can be associated with each of the assessments based on your business needs. You can define scope of the assessment in terms of business entities or domains such as business processes, applications, and assets. Assessment scoping ensures that the necessary data is collected in effective and efficient manner for risk evaluation.

Risk is calculated based on various factors such as significance of a specific question, associated response, assigned assets and their importance (ranking), mapped threats and events, and other such criteria that are defined as part of customization of the questionnaire. For more information about creating a question, see "Questionnaire Builder" on page 170.

Procedure

1. Create an assessment program by selecting a non-GDPR framework (non-PRA framework), for example, ISO framework to create your assessment. For the steps on how to create an assessment program, see "Creating an assessment program" on page 177.

   On the **Create Assessment** page topics, subtopics, and factors that are associated with the framework that you selected are displayed.
2. Select topics and subtopics from the list.
3. Include entities and concepts for each of the assessments (topics) that you selected.
   a) Click the **Edit Assessment** icon ✎.
   b) Select the necessary entities. By default, all the entities are selected.
   c) For each of the selected entities, associate necessary scopes. To select scopes, click the **Select Scope** icon ⌄ .
   d) To save the changes, click the save icon 💾.
4. Click **Create Assessment**.

What to do next

Assign resources to the assessment that you created. For the steps on how to assign resources, see "Assigning resources to run assessment" on page 179.

Assigning resources to run assessment

Assign resources to run various tasks that are related to assessments.

About this task

The resources are assigned to the following roles.

Administrator

Creates assessment programs, individual assessments within a program, assessment templates, and related questions, assignment of users for providing responses to assessments.

Assessor
Provides responses to individual assessments within a program.

Approver
Reviews and approves assessment responses.

By using the IBM Data Risk Manager user management function, administrators can create users, assign user roles, update user information, and change a user password. For more information about user management, see "Managing users" on page 89.

Procedure

1. Create an assessment program. For the steps on how to create an assessment program, see "Creating an assessment program" on page 177.
2. Create an assessment. For the steps on how to create an assessment, see "Creating an assessment for GDPR framework" on page 178 or "Creating an assessment for non-GDPR framework" on page 179.
3. On the **Assign Resource** page, select resources from the **Assign Resource** list for assigning to the user roles such as Administrator, Assessor, and Approver.
4. Select **Assign resources to all assessments** to assign the selected resources for all the individual assessments.
5. Click **Assign Role**.

What to do next

Run the assessment tasks. For the steps on how to run an assessment, see "Performing an assessment" on page 180.

Performing an assessment

The user with Assessor role must provide responses to assessment questionnaires. After responses are provided to the questions, the Assessor submits assessment to the Approver for review and approval.

Before you begin

- An IBM Data Risk Manager program is created with defined scope and users are provisioned for accessing the program.
- Users are created with appropriate privileges within IBM Data Risk Manager.
  - For users who are designated as Assessment Program administrators, assign `BCM Administrator` role
  - For users who are designated to provide responses for an assessment, assign `C3 Assessment General` role.

About this task

Responses to some questions lead to further questions. You can express this relationship by creating a conditional relationship between questions. In a conditional relationship, there is a parent question and a child question. The child question is, by default, not displayed. The child question is displayed only when an enabling response is provided to the parent question. By using the decision tree, you can quickly view and identify the relationships between the questions.

Decision tree is a hierarchical structure with nodes and directed edges. A decision tree typically starts with a single node (parent question), which branches (child questions) into possible outcomes. Each of those outcomes can lead to additional nodes, which branch off into other possibilities. This gives it a tree-like structure. By using a decision tree, you can easily explain the decisions, identify possible events that might occur, and see potential outcomes.

For non-PRA assessments, when you are providing response to a question, context data can be captured based on the defined entities (scopes) for risk score calculation. For more information about how to define entities and associate them with the assessments, see "Creating an assessment program" on page 177 and "Creating an assessment for non-GDPR framework" on page 179.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`) by using your Assessor credentials.
2. Click the notifications icon to display Message Dashboard.

   The notifications include a link to the assessment program or the individual assessment for which the responses are to be provided.
3. Alternatively, click the application menu icon .
4. Click **Assessment**.
5. Select the assessment program from **Assessment Program List**. List of assessments that are associated with the assessment program is displayed in the **Assessments** section.
6. Select the assessment for which you must provide responses.

   The following list provides more information to perform the assessment.

   - Click the **Assign Resource** icon to assign resources.
   - Click the **Compute Assessment Score** icon to compute score for non-PRA assessment.
   - Click the **Notes** icon to add a note about the assessment.
   - Click the **Import Assessment** icon to import responses from a completed assessment. After an assessment response is imported, the assessment gets locked and cannot be edited.

     An assessment program is available for sharing only after it is signed-off, and the option **Can be Shared** is selected when assessment program is created.
   - Click the **Delete Assessment** icon to delete the selected assessment.
   - Click the **Manage Scope** icon to add or modify your scope selection for the non-PRA assessments.

     You can modify and manage the scope selection that you defined during assessment creation. Only the owner of assessment program or assessment author can modify the scope selection. You can modify scope selection only for the assessments with status such as `Ongoing`, `Paused`, and `Completed`.
   - The assigned icon indicates that you are the Assessor for the assessment.
7. Click **Launch Assessment** to start the assessment.
8. Register items are displayed on the left pane. Select a register item from the list. The associated questions are displayed.

   Click the icon to exclude the selected registry item for assessment. When a registry item is excluded from the assessment, the Assessor cannot include the item again. The approver can include this item back, if necessary.

   For non-PRA assessments, the **Context** icon is displayed to select the context information. Click the context icon to select context at registry item (control) level. The same context information is applicable to all the associated questions.

   - Click **Grid View** to view the assessment questions and responses in grid format (default view).
   - Click **List View** to view the assessment questions and responses in list format.

9. Select a question and specify your response, notes, and observation about the response. Click the more options icon ••• to provide the following information.
    - Click **Notes** to add a note about the response.
    - Click **Observation** to select your answer observations.
10. Add following details for the questions.
    - Click the **Notes** icon to add a note about the question.
    - Click the **Audit Trails** icon to view the audit trails.
    - If you want to reset a response value, click the **Reset** icon ↻ to default values.
    - For non-PRA assessments, click the **Context** icon ◉ to add or update context information.

      The **Context** icon is displayed only after response to the question is provided. Select the contexts and save the information based on your needs. If the contexts are already selected at control level, you can modify the details if needed.
11. Specify responses to all the questions.
12. Click **Submit for Review** to submit the assessment for review to validate the responses.
13. Click **Yes** on the confirmation window.

    After the assessment is submitted for review, changes to the responses cannot be made until the assessment approver validates the responses.

What to do next

Approver is notified about the completion to review and approve assessment responses. If necessary, the Approver can add comments and send back the assessment to Assessor for further modification. For more information about approving responses, see “Completing review and approving assessment responses” on page 182.

Completing review and approving assessment responses

The Approver must review and approve assessment responses. If necessary, the Approver can add review comments and send back the assessment to Assessor for further modifications.

Before you begin

- An IBM Data Risk Manager program is created with defined scope and users are provisioned for accessing the program.
- Users are created with appropriate privileges within IBM Data Risk Manager.
    - For users who are designated as Assessment Program administrators, assign `BCM Administrator` role
    - For users who are designated to provide responses for an assessment, assign `C3 Assessment General` role.

About this task

Responses to some questions lead to further questions. You can express this relationship by creating a conditional relationship between questions. In a conditional relationship, there is a parent question and a child question. The child question is, by default, not displayed. The child question is displayed only when an enabling response is provided to the parent question. By using the decision tree, you can quickly view and identify the relationships between the questions.

Decision tree is a hierarchical structure with nodes and directed edges. A decision tree typically starts with a single node (parent question), which branches (child questions) into possible outcomes. Each of those outcomes can lead to additional nodes, which branch off into other possibilities. This gives it a tree-like shape. By using a decision tree, you can easily explain the decisions, identify possible events that might occur, and see potential outcomes.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) by using your Approver credentials.
2. Click the notifications icon ✉ to display Message Dashboard.

   The notifications include a link to the assessment program or the individual assessment for which the responses are to be provided.
3. Alternatively, click the application menu icon .
4. Click **Assessment**.
5. From **Assessment Program List**, select the assessment that you need to review and provide review comments.
6. Click the **Launch Assessment** icon to open the assessment page for reviewing responses and adding review comments. By default, all the questions with responses are displayed. You can also view the questions based on the group that is associated with the question.
   - Click **Grid View** to view the assessment questions and responses in grid format (default view).
   - Click **List View** to view the assessment questions and responses in list format.
7. Review responses of all the questions.
   - Click the **Notes** icon to view comments about a question.
   - Click the **Audit Trails** icon to view the audit trail information.
   - Hover on **Answered** to view the computed score for a specific question.
   - Click the **Review Comments** icon to add review comments.
   - Click the **More Options** icon ••• to view response information.
     - Click the **Notes** icon to view the note that was added when the responses are provided.
     - Click the **Observation** icon to view the observation data.

   .
8. To view all the comments from reviewer or accessor for an assessment, enable the **Comment Mode** toggle button and click **Comments**.
   - Click **History** to view the all comments of accessor or reviewer.
   - Click **Review Sheet** to accept or reject the comments.
9. If you need to send the assessment to Assessor for further modifications, click **Back to Assessor**.
10. Click **Complete Review** to complete the review process.
11. In the **Complete Review** window, provide your comments about review completion.
12. Click **Submit**.
13. Click **OK** on the **Information** window.

What to do next

After the review process is completed, the Approver can sign off to complete the assessment. For the steps on how to sign off, see "Signing-off an assessment program" on page 184.

Signing-off an assessment program

The Approver must sign off to complete the assessment.

Before you begin

Ensure that the review of assessment responses is complete.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) by using your Approver credentials.
2. Click the notifications icon ✉ to display Message Dashboard.

   The notifications include a link to the assessment program or the individual assessment for which the responses are to be provided.
3. Alternatively, click the application menu icon ⠿.
4. Click **Assessment**.
5. In the **Assessment Program List** section, select the assessment that you need to sign off.
6. Click the **More options** icon •••, and then click **Sign-off**.
7. In the **Sign-off assessment program** window, provide your comments about assessment sign off.
8. Click **Submit** to complete the sign-off process.

Viewing assessment scorecard report

Results of the independent assessments generate a risk assessment report based on the responses that are obtained. On the Assessments dashboard, you can view the assessment information in graphical and tabular format. Graphical representation of data helps you to easily understand and interpret information.

About this task

You can download reports for Information Asset Register, Vulnerability Controls, and Risk Assessment.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) by using your Approver credentials.
2. Click the notifications icon ✉ to display Message Dashboard.

   The notifications include a link to the assessment program or the individual assessment for which the responses are to be provided.
3. Alternatively, click the application menu icon ⠿.
4. Click **Assessment**.
5. To view report for GDPR (PRA) framework assessment, run the following steps.
   a) Select the assessment program from **Assessment Program List**.
   b) Select the completed assessment for which you want to view the report.
   c) Click the **Report** tab.
   d) Click the **Refresh view** icon ⟳ to refresh view for displaying graphical report for the selected assessment.
   e) Click the **Toggle Chart/Grid view** icon to ▦ display information about the assessment in a tabular format.
   f) For the expanded view, click the **Expand/Collapse** icon ↗.

g) To configure the risk remediation actions, run the following steps.

   1) Click the **Risk Assessment** tab.

   2) Select a risk.

   3) Click the **Update action** icon to select an action for remediating risks.

   4) Click the **Create Activity** icon to define the risk remediation actions. For information about how to create activities and tasks in Action Center, see "Creating a remediation activity" on page 142.

h) Click **Download Report** to download the reports for **Risk Assessment**, **Information Asset Register**, and **Vulnerability Controls**.

6. To view report for non-GDPR Framework assessment, run the following steps.

   a) Select the assessment program from **Assessment Program List**.

   b) Select the completed assessment for which you want to view the report.

   c) Click the **Compute assessment score** icon .

   d) Click the **Report** tab.

   e) Click the **Refresh view** icon to refresh view for displaying graphical report for the selected assessment.

   f) Click the **Toggle Chart/Grid view** icon to display information about the assessment in a tabular format.

   g) For the expanded view, click the **Expand/Collapse** icon .

What to do next

For a non-PRA assessment, you can also view scope-based assessment report for the scopes that are defined when you created the assessment program. For more information about how to view the report, see "Viewing scope-based assessment report" on page 185.

Viewing scope-based assessment report

On the Assessment dashboard, you can view results of the independent assessments that are performed on a framework against a set scopes (business entities) that you defined. Graphical representation of data helps you to easily understand and interpret information.

About this task

For non-PRA assessments, when you are providing response to a question, context data can be captured based on the defined entities (scopes) for risk score calculation. For more information about how to define entities and associate them with the assessments, see "Creating an assessment program" on page 177 and "Creating an assessment for non-GDPR framework" on page 179. Assessment scoping ensures that the necessary data is collected in effective and efficient manner for risk evaluation.

Risk score on the report represents the average score of the controls for the defined scopes.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) by using your Approver credentials.

2. Click the notifications icon to display Message Dashboard.

   The notifications include a link to the assessment program or the individual assessment for which the responses are to be provided.

3. Alternatively, click the application menu icon .

4. Click **Assessment**.
5. Select the assessment program from **Assessment Program List**. You can view the scope-based assessment report only for non-PRA framework.
6. Select the completed assessment for which you want to view the report.
7. Click the **Compute Assessment Score** icon .
8. Click the **Scope Based Report** tab.

   The tabs are displayed for the entities that you defined during assessment program creation for viewing scope-based assessment data. For example, Business Processes, Applications, or Data Sources.
9. To the view the report for business process entity, click the **Business Processes** tab.
10. To the view the report for application entity, click the **Applications** tab.
11. To the view the report for data source entity, click the **Data Sources** tab.

Assessment Outcome Management

Based on non-PRA assessment results, appropriate actions can be implemented to address and mitigate the identified risks. You can use the Assessment Outcome Management module of IBM Data Risk Manager to view and manage risks.

Adding a risk

You can create risks, define their attributes, and add remediation plans for a scope based on the risk score that is generated after risk evaluation of non-PRA assessment is completed. Multiple risks can be added to a scope.

About this task

You can import risk attributes from IBM Data Risk Manager threat inventory. For more information about threat inventory, see "Threat inventory" on page 122.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`) by using your Approver credentials.
2. Click the application menu icon .
3. Click **Assessment**.
4. Select an assessment program for on-PRA framework from **Assessment Program List**.
5. Click the **Assessment Outcome Management** icon .
6. Select a scope from the list.
7. Click **Add Risk**.
8. On the **Add Risk** window, set the following options.

   a) Specify the risk attributes.

Risk Name	Specify a name for the risk.
Category	Specify the category that the risk belongs to.
Risk Type	Specify the classification of the risk.
Criticality	Specify the criticality level of the risk.
Impact Level	Specify the level of risk impact, low, medium, or high.
Probability	Specify the likelihood of the risks that are occurring.

Risk Description	Add a description of the risk.

   b) Alternatively, you can import risk attributes from IBM Data Risk Manager threat repository.

      1) Click **Threat Repository**.

      2) Select a threat from the list.

   c) Specify the scope attributes.

Status	Specify the status of the risk.
Requested Exception	Specify the exception information to compliance.
Deadline to Fix	Specify the planned risk mitigation date.
Mitigation Date	Specify the actual risk mitigation date.
Mitigation	Specify the risk mitigation information.
Risk Remarks	Specify risk remarks.

9. Click **Save**.

What to do next

Add a remediation activity for the risk that you now created. For the steps on how to create an activity, see "Creating an action plan to remediate risks" on page 187.

Creating an action plan to remediate risks

You can add remediation activities for the identified assessment risks.

Before you begin

Ensure that the assessment evaluation is completed, risk score is generated, and risks are identified for the scopes. For the steps on how to add risks, see "Adding a risk" on page 186.

About this task

You can use predefined remediation activities and tasks that are imported from a solution package for defining action plans. Click the predefined activities icon 🛠 to select the predefined activities.

Procedure

1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`) by using your Approver credentials.
2. Click the application menu icon ⠿.
3. Click **Assessment**.
4. Select an assessment program for on-PRA framework from **Assessment Program List**.
5. Click the **Assessment Outcome Management** icon 🛡.
6. Select a scope from the list. Associated risks are displayed under **Identified Risks**.
7. Select a risk for that you need to create an activity.
8. Click **Add Activity**.
9. On the **Create Remediation Activity** window, specify the necessary details.

Option	**Description**
Activity Name	Specify the activity name.
Status	Specify the activity status, for example, `Yet to Start`, `In Progress`, or `Completed`.

Option	Description
Activity Operation	Select an operation activity from the list.
Associated Risk	Select a data source from the data source inventory for which you need create a remediation activity. You can assign only one data source as scope to an activity.
Start Date	Specify the date to start the remediation activity.
End Date	Specify the date to end the remediation activity.
Duration	Specifies the duration between activity start and end date.
Impact	Specify the level of risk impact, low, medium, or high.
Urgency	Specify the urgency level to address the risk.
Priority	Specify the priority level in which the risk needs to be resolved, based on impact and urgency.
Severity	Specify the severity level of the risk.
Sub Category	Specify the risk sub category.
Description	Add a description of the risk.
Category	Specify the category that the risk belongs to.
Contact Type	Specify the contact type.
Assigned Resources	Specify the risk owner.

10. To save the activity details, click **Create**.

What to do next

Further edit and manage the activity that you created with more details in the Action Center component of IBM Data Risk Manager. In Action Center, you can view and access the activity under **Risk Remediation Project** for modifications. For more information about Action Center, see "Action Center" on page 140.

Diagnostic tools

Diagnostic tools are available to help you troubleshoot issues and resolve problems that are encountered when you are working with IBM Data Risk Manager.

Integration Diagnostics Tool

IBM Data Risk Manager includes a diagnostic tool that can be used to assist you with problem determination.

Integration Diagnostics Tool in IBM Data Risk Manager helps to troubleshoot the database and integration connectivity issues.

1. Open a command prompt /terminal.
2. SSH into IBM Data Risk Manager.
3. Run the following command.

```
cd ~/Diagnostics
java -jar a3IntegrationDiagnostics.jar
```

4. The following output is displayed for you to select an option.

```
Welcome to iDRM Diagnostics Tool
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Please enter a valid input
 Below are the choices.
 1. Integration
 2. Datasource
 3. Exit
```

5. To identify and resolve the integration issues, type 1, and press **Enter**.
6. To identify and resolve the database connectivity issues, type 2, and press **Enter**.

Note: For more information about the errors that are reported, check the logs files.

Health Diagnostics Tool

IBM Data Risk Manager includes Health Diagnostics Tool that can be used to assist you with problem determination.

Health Diagnostics Tool in IBM Data Risk Manager helps you to monitor server health, agent health, license validity status, patch status, and OAuth token generation validity.

1. Open a command prompt /terminal.
2. SSH into IBM Data Risk Manager.
3. Run the following command.

```
cd ~/Diagnostics
java -jar a3HealthDiagnostics.jar
```

4. The following output is displayed for you to select an option.

```
Welcome to iDRM Health Diagnostics
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Here are your options. Please enter a valid option
Press 1 to check the server health
Press 2 to check Microservices health
Press 3 to check if license is up-to-date
Press 4 to check oauth token generation
Press 5 to check the status of the patch
Press 6 to exit
```

5. Type the number that is displayed next to your choice and press **Enter**.

Note: For more information about the errors that are reported, check the logs files.

Troubleshooting and support

Troubleshooting and support information for IBM Data Risk Manager helps you understand, isolate, and resolve problems.

The troubleshooting section includes descriptions of the events that generated the problems, the symptoms, the environment, the possible causes, and suggestions for recovery actions.

The support section provides information about the tools and options that you can use to connect to the service and support organization. The support section also includes general information about searching knowledge bases, getting fixes, and contacting IBM support, as well as product-specific topics.

To resolve a problem on your own, you can find out how to identify the source of a problem, how to gather diagnostic information, where to get fixes, and which knowledge bases to search. If you need to contact IBM Support, you can find out what diagnostic information the service technicians need to help you address a problem.

General information

To get started with troubleshooting, familiarize yourself with the basic techniques for troubleshooting and on how to contact and exchange information with IBM Support. You can also use tools such as IBM knowledge base, Fix Central, and Support Portal.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multisite installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running in an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the IBM Data Risk Manager documentation. However, sometimes you need to look beyond the documentation to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Search for content by using the IBM Support Assistant (ISA).

  ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.

- Find the content that you need by using the IBM Support Portal.

  The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.

- Search for content about IBM Data Risk Manager.

  – IBM Data Risk Manager Support website.

- Search for content by using the IBM masthead search.

  You can use the IBM masthead search by typing your search string into the **Search** field at the top of any ibm.com® page.

- Search for content by using any external search engine, such as Google, Yahoo, or Bing.

  If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

  Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

Getting fixes from Fix Central

You can use Fix Central to find the fixes that are provided by IBM Support for various products, including IBM Data Risk Manager. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. A product fix might be available to resolve your problem.

About this task

Procedure

To find and install fixes:

1. Obtain the tools that are required to get the fix. If it is not installed, obtain your product update installer. You can download the installer from Fix Central.

   This site provides download, installation, and configuration instructions for the update installer.
2. Select IBM Data Risk Manager as the product, and select one or more check boxes that are relevant to the problem that you want to resolve.

   For details, see: http://www.ibm.com/systems/support/fixes/en/fixcentral/help/faq_sw.html.
3. Identify and select the fix that is required.
4. Download the fix.
   a) Open the download document and follow the link in the "Download Package" section.
   b) When you download the file, ensure that the name of the maintenance file is not changed.

      This change might be intentional, or it might be an inadvertent change that is caused by certain web browsers or download utilities.
5. Apply the fix.
   a) Follow the instructions in the "Installation Instructions" section of the download document.
   b) For more information, see the "Installing fixes with the Update Installer" topic in the product documentation.

Exchanging information with IBM

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Sending information to IBM Support

To reduce the time that is required to resolve your problem, you can send trace and diagnostic information to IBM Support.

Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR).
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data manually or automatically:
   - Collect the data manually.
   - Collect the data automatically.
3. Compress the files by using the `.zip` or `.tar` file format.
4. Transfer the files to IBM.

   You can use one of the following methods to transfer the files to IBM:

   - IBM Support Assistant
   - The Service Request tool
   - Standard data upload methods: FTP, HTTP
   - Secure data upload methods: FTPS, SFTP, HTTPS
   - Email

   All of these data exchange methods are explained on the IBM Support website.

Receiving information from IBM Support

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as `anonymous`. Use your email address as the password.
2. Change to the appropriate directory:

   a) Change to the `/fromibm` directory.

   ```
   cd fromibm
   ```

   b) Change to the directory that your IBM technical-support representative provided.

   ```
   cd nameofdirectory
   ```

3. Enable binary mode for your session.

   ```
   binary
   ```

4. Use the **`get`** command to download the file that your IBM technical-support representative specified.

```
get filename.extension
```

5. End your FTP session.

```
quit
```

Subscribing to Support updates

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

About this task

By subscribing to receive updates about IBM Data Risk Manager, you can receive important technical information and updates for specific IBM Support tools and resources. You can subscribe to updates by using one of two approaches:

RSS feeds

For information about RSS, including steps for getting started and a list of RSS-enabled IBM web pages, visit the IBM Software Support RSS feeds site.

My Notifications

With **My Notifications**, you can subscribe to Support updates for any IBM product. **My Notifications** replaces **My Support**, which is a similar tool that you might have used in the past. With **My Notifications**, you can specify that you want to receive daily or weekly email announcements. You can specify what type of information you want to receive (such as publications, hints and tips, product flashes (also known as alerts), downloads, and drivers). **My Notifications** enables you to customize and categorize the products about which you want to be informed and the delivery methods that best suit your needs.

Procedure

To subscribe to Support updates:

1. Subscribe to My Notifications by going to the IBM Support Portal and click **My Notifications** in the **Notifications** portlet.
2. Sign in using your IBM ID and password, and click **Submit**.
3. Identify what and how you want to receive updates.
   a) Click the **Subscribe** tab.
   b) Select the appropriate software brand or type of hardware.
   c) Select one or more products by name and click **Continue**.
   d) Select your preferences for how to receive updates, whether by email, online in a designated folder, or as an RSS or Atom feed.
   e) Select the types of documentation updates that you want to receive, for example, new information about product downloads and discussion group comments.
   f) Click **Submit**.

Results

Until you modify your **RSS feeds** and **My Notifications** preferences, you receive notifications of updates that you have requested. You can modify your preferences when needed (for example, if you stop using one product and begin using another product).

Related information

IBM Software Support RSS feeds

Subscribe to My Notifications support content updates

My Notifications for IBM technical support

My Notifications for IBM technical support overview

Log files to troubleshoot problems

IBM Data Risk Manager generates log files that you can use to troubleshoot problems.

You can use the log files to check health status of micro services that are configured with IBM Data Risk Manager.

For more information about Diagnostics tools, see "Diagnostic tools" on page 188.

Viewing the log files

1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
2. Click the application menu icon ⠿.
3. Click **Administration**.
4. On the **Administration** page, click **Diagnostics**.
5. From the **Instance Health** section, select the micro service for which you want to view the log files.
6. To view the log file contents, click **Logs**.
7. To download the log files, under **Download Multiple Logs**, select the file and then click **Download**.
8. Review the operational logs.
9. Contact IBM support if the error messages are logged.

Product installation problems and workaround

Troubleshoot problems that might occur during IBM Data Risk Manager installation.

Micro services are not running

Problem	Micro services are not running after the installation of IBM Data Risk Manager.
Cause	Incorrect usage of host name when IBM Data Risk Manager is installed and configured.

Resolution	1. Connect to IBM Data Risk Manager Server over Secure Shell (SSH).
	SSH is an encrypted network protocol to securely connect to the IBM Data Risk Manager Server.
	2. From the command line, run the following command to check health status of the micro services that are configured with IBM Data Risk Manager.
	`service dbscanner status`
	`service guardium status`
	`service idmanager status`
	`service listener status`
	`service symantec status`
	3. Run the following commands to start the micro services that are not running. Ensure that the service is stopped before you start the service.
	`service dbscanner start`
	`service guardium start`
	`service idmanager start`
	`service listener start`
	`service symantec start`

Configuration problems and workaround

Troubleshoot problems that might occur when you integrate IBM Security Guardium with IBM Data Risk Manager to import data sources.

Connection failure error during IBM Security Guardium configuration

Problem	You might encounter connectivity issues when you integrate IBM Security Guardium with IBM Data Risk Manager.
Cause	The connection failure might occur for any of the following reasons: • Incorrect URL usage to connect to IBM Security Guardium. • IBM Security Guardium micro service might not be running. • Incorrect credentials are provided to connect to IBM Security Guardium.

Resolution	**Specifying the correct URL**
	1. Log on to IBM Data Risk Manager Application Suite (`https://`*<IDRM-Server-IP-Address>*`:8443/albatross/a3suite`) as `admin` user.
	2. Click the application navigation icon ⠿.
	3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
	4. Under **Adapter Configuration**, click **IBM Guardium**.
	5. Under **Integration Instances**, select the IBM Security Guardium instance that needs the URL correction.
	6. Under **Instance Details**, specify the correct URL in the **URL** field.
	7. Click **Test Connection** to test whether the communication between IBM Security Guardium instance and IBM Data Risk Manager is successful.
	8. Click **Save**.
	Checking whether the micro service is running
	1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://`*<IDRM-Server-IP-Address>*`:8443/albatross/a3suite`).
	2. Click the application menu icon ⠿.
	3. Click **Administration**.
	4. On the **Administration** page, click **Diagnostics**.
	5. Check whether the IBM Security Guardium micro service is running. If the service is stopped, run the following command to check the status.
	a. Connect to the server over SSH.
	b. From the command line, run the following command.
	`service guardium status`
	6. If the service is stopped, run the following command to start the service.
	`service guardium start`
	Specifying the correct credentials
	1. Log on to IBM Data Risk Manager Application Suite.
	2. Click the application navigation icon ⠿.
	3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
	4. Under **Adapter Configuration**, click **IBM Guardium**.
	5. Under **Integration Instances**, select the IBM Security Guardium instance for which the correct credentials must be specified.
	6. Under **Instance Details**, specify the correct user name and password in the **User Name** and **Password** fields.
	7. Click **Save**.

User administration problems and workaround

Troubleshoot problems that are related IBM Data Risk Manager login and user permissions.

Unable to log on IBM Data Risk Manager

Term	Detail
Problem	Unable to log on to IBM Data Risk Manager with the specified credentials.
Cause	The connection failure might occur for any of the following reasons: • User account is locked. • User account is disabled. • Account password is expired.
Resolution	**Unlocking a user account** 1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) with administrator privileges. 2. Click the application navigation icon ⠿. 3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **User**. 4. From the **Application Users** list, select the user name. 5. Clear the **Account Locked** check box. 6. Click **Save**. **Enabling the user account** 1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **User**. 2. From the **Application Users** list, select the user name. 3. Select the **Enable User** check box. 4. Click **Save**. **Changing password** 1. Go to the IBM Data Risk Manager**Sign In** page. 2. Click the **Change Password** option. 3. Update the password. 4. Click **Change**.

Unable to access IBM Data Risk Manager menu options

Problem	Some of the IBM Data Risk Manager menu options are not available.
Cause	The permissions that are associated with the user account limit the navigation of the user interface. Some of the menu options might not be available based on the assigned roles.

Resolution	1. Log on to IBM Data Risk Manager Application Suite with administrator privileges. 2. Click the application navigation icon ⠿. 3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **User**. 4. From the **Application Users** list, select the user name who requires access to the menu options. 5. In the **Roles** section, select a role. 6. Click **Save**.

Data source management problems and workaround

Troubleshoot problems that occur when you add data sources to IBM Data Risk Manager and discovering data sources.

Connectivity issues when data sources are added to IBM Data Risk Manager

Problem	Data sources are not imported or saved in IBM Data Risk Manager.
Cause	The data source import problems might occur if you specify incorrect values for any of the following database connection parameters. • Database credentials • IP address or port information • Database name
Resolution	Ensure that the specified database connection parameters are correct. 1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`). 2. Click the application navigation icon ⠿. 3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory**. 4. Select **Data Source**. The data source list is displayed. 5. Search and locate your data source. 6. On the selected data source, click the Actions icon ⋯ . 7. To edit database connection information, click the edit icon ✎. 8. Update database connection information. 9. Click **Add**.

Unable to run data source discovery operation

Problem	Native discovery of data sources does not work. When native discovery is run, the scan is in Queued status.
Cause	Network Mapper (NMAP) might not be installed on the server.

Resolution	Check whether NMAP is installed on the server.
	1. Connect to the server over SSH.
	2. Run the following command in a command line to know the NMAP location.
	`whereis nmap`
	If NMAP is installed, the path is displayed as `/usr/local/nmap`.
	3. Run the following command to know the NMAP version.
	`Nmap –version`
	4. If no results are returned for the commands, contact IBM customer support to resolve the issue.

Program management problems and workaround

Troubleshoot problems that occur during IBM Data Risk Manager program creation and management.

Programs are not visible in the dashboard

Problem	IBM Data Risk Manager programs are not visible in the dashboard.
Cause	User is not entitled to access the programs.
Resolution	Ensure that the user is associated with a program. 1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`) with administrator privileges. 2. Click the application navigation icon ⠿. 3. Click **Business Context Modeler**. Program list is displayed in the **Program Portfolio** page. 4. Select the program to which you want associate a user and click the program name to edit the program. 5. Click the **Scope** icon. 6. Select the user name. 7. Click **Assign**.

Visualizer plots business context data incorrectly

Problem	Expected business context data cannot be plotted on IBM Data Risk Manager Visualizer. For example, applications within the program scope cannot be plotted on the visualizer.
Cause	The relevant business context data might not be included within the program scope.

Resolution	Ensure that relevant business context entities are added to the program scope. 1. Log on to IBM Data Risk Manager Application Suite with administrator privileges. 2. Click the application navigation icon ⠿. 3. Click **Business Context Modeler**. 4. Select the program to which you want to include business context data and click the program name to edit the program. 5. Click the **Scope** icon. 6. Under **Scope**, select the business context entities for `LOB`, `Application`, `Platform`, `Compliance`, `Environment`, `Resource`, and `Data Source`. 7. Click **Assign**.

Program scope selection set does not include all the imported business context data

Problem	All the imported business context data is not available when you set up the program scope.
Cause	Imported context data does not have the correctly mapped set of values.
Resolution	Review the CSV files for `Database`, `Application`, and `Business Process` data sets, and validate whether the data set is correctly mapped. For more information about business context data, see "Mapping business context data" on page 99.

Business context modeling problems and workaround

Troubleshoot problems that occur when you import business context data into IBM Data Risk Manager server.

Importing business context data failed

Problem	The error message `Internal Server Error` is displayed when the context data is imported.
Cause	• The CSV files that are used to import the data might be corrupted. • Incorrect import jobs are blocking the import operation.

Resolution	**Checking whether the CSV files are corrupted** 1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`). 2. Click the application navigation icon ⠿. 3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**. 4. Click the CSV file icon CSV to select `Database`, `Application`, and `Business Process` CSV files. 5. Click **Load**. 6. Review the files and validate correctness of data. 7. If the CSV files are not loaded in tabular format, update the files. 8. Reload the files. **Checking whether the import jobs are blocked** 1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`). 2. Click the application menu icon ⠿. 3. Click **Administration**. 4. Click the **Manage Load Transactions** tab. 5. Identify the transaction type that is identified as `IMPORT_WIZARD`. 6. Click **Remove Transaction** to cancel the transaction operation. 7. Reload the context data.

Cannot import context data due to mapping conflict

Problem	Unable to import the context data. In the preview, a few columns on the data sheet are displayed in red.
Cause	• The CSV files that are used to import the data might be corrupted. • In the updated business context data sheets that are loaded, context data attributes might have changed.

Resolution	**Checking whether the CSV files are corrupted** 1. Log in to IBM Data Risk Manager. 2. Click the application navigation icon ⠿. 3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**. 4. Select the `Database`, `Application`, and `Business Process` CSV files. 5. Click **Load**. 6. Review the files and validate correctness of data. 7. If the CSV files are not loaded in tabular format, update the files. 8. Reload the files. **Removing the transaction and reloading context data** 1. Log in to IBM Data Risk Manager Administration. 2. Click the **Manage Load transactions** tab. 3. Identify the transaction type that is identified as `IMPORT_WIZARD`. 4. Click **Remove Transaction** to cancel the transaction operation. 5. Reload the context data.

Loading the context data CSV file is failed

Problem	When the context data CSV file is loaded, the following error message is displayed. `Wrong file format. Please select only CSV file format.`
Cause	The CSV file type was interpreted by windows as undefined.

Resolution	1. Add the following contents to a text file and save the file with a name `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. Rename the file with a name `csv_import_config.reg`.
	3. Copy the file `csv_import_config.reg` file to all the systems where IBM Data Risk Manager is installed.
	4. Double-click the `csv_import_config.reg` file.
	5. Click **Yes** to confirm the changes in the registry files.
	The configuration file adds the file type as `text/csv`.
	6. Load the context data CSV files to import.

Solution packages import problems and workaround

Troubleshoot problems that occur when you import solution packages into IBM Data Risk Manager Server.

Importing a solution package failed

Problem	Following error message is displayed when the solution package is imported. `Failed to save data`
Cause	- The CSV files that are used to import the solution package might be corrupted. - Incorrect import jobs are blocking the import operation.
Resolution	**Checking whether the CSV files are corrupted** 1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`). 2. Click the application navigation icon ⠿. 3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Solution Package**. 4. Click **Browse** to select the CSV files for **Solution Package**, **Policies**, and **Tasks** to load. 5. Review and validate the correctness of data. 6. Update the files if necessary. 7. Reload the files. **Checking whether the import jobs are blocked** 1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`). 2. Click the application menu icon ⠿. 3. Click **Administration**. 4. On the **Administration** page, click **Manage Load transactions**. 5. Identify the transaction type that is identified as `IMPORT_WIZARD`. 6. Click **Remove Transaction** to cancel the transaction operation. 7. Reload the context data.

IBM Security Guardium classifier policy is not found in Policy Central

Problem	The IBM Security Guardium classifier policy that was imported as a solution package is not available in **Policy Management Central**.
Cause	The policy was not deployed in IBM Security Guardium.

Resolution	Deploying the policy in IBM Security Guardium. 1. Go to **Business Context Modeler** > **Policy Management Central**. 2. Search for the missing policy under **Data Discovery and Classification**. 3. After the policy is located, click **Deploy**. 4. Select **IBM Guardium** from the list. 5. Click **OK** to deploy the policy in IBM Security Guardium.

Policy management problems and workaround

Troubleshoot problems that occur during policy creation and management.

Error message while importing policies

Problem	Importing policies from IBM Security Guardium is failed.
Cause	• Unsuccessful import job. • Incorrect configuration of IBM Security Guardium. • IBM Security Guardium micro service is not running.

Resolution	**Removing the transaction and reimporting policies**
	1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
	2. Click the application menu icon ⠿.
	3. Click **Administration**.
	4. On the **Administration** page, click **Manage Load transactions**.
	5. Identify the transaction type that is identified as `POLICIES`.
	6. Click **Remove Transaction** to cancel the transaction operation.
	7. Import the policies again.
	Verifying IBM Security Guardium configuration
	1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**.
	2. Select **IBM Guardium**.
	3. Review the configuration details and update as necessary.
	4. To verify the connectivity, click **Test Connection**.
	5. Click **Save** after the successful connection to IBM Security Guardium.
	Verifying IBM Security Guardium micro service status
	1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
	2. Click the application menu icon ⠿.
	3. Click **Administration**.
	4. On the **Administration** page, click **Diagnostics**.
	5. Check whether the IBM Security Guardium micro service is running. Run the following command to check the status.
	a. Connect to the server over SSH.
	b. From the command line, run the following command.
	`service guardium status`
	6. If the service is stopped, run the following command to start the service.
	`service guardium start`

Data discovery problems and workaround

Troubleshoot problems that occur during data discovery.

Data source is not found in the inventory

Problem	Data source is not found in the data source inventory, and not available for scanning.
Cause	Data source is not included within the scope of the program.

Resolution	Ensure that the data source is added to the program scope. 1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) with administrator privileges. 2. Click the application navigation icon ⠿. 3. Click **Business Context Modeler**. The list of program is displayed in the **Program Portfolio** page. 4. Select the program and click the program name to edit the program. 5. Click the **Scope** icon. 6. Under **Scope**, click the **Data Source** icon. 7. Select the data sources. 8. Click **Assign**.

IBM Security Guardium classifier policy is not found in Security Command and Control Center

Problem	IBM Security Guardium classifier policies that are imported as a solution package are not available in Policy Central to run the scan.
Cause	Policy was not deployed in IBM Security Guardium.
Resolution	Ensure that the policy is deployed in IBM Security Guardium. 1. Go to **Business Context Modeler** > **Policy Management Central**. 2. Search for the missing policy under **Data Discovery and Classification**. 3. After the policy is located, click **Deploy**. 4. Select **IBM Guardium** from the list. 5. Click **OK** to deploy the policy in IBM Security Guardium.

IBM Security Guardium classifier scan failed

Problem	IBM Security Guardium classifier scan is failed.
Cause	• Incorrect data source credentials • Data source is deleted in IBM Security Guardium • Policy is deleted in IBM Security Guardium.

Resolution	**Verifying and correcting database connection information** 1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory**. 2. Select **Data Source**. The data source list is displayed. 3. Search and locate your data source. 4. Select the data source and click the Actions icon ••• 5. Click the edit icon ✎ to update database connection information. 6. Click **Save**. **Creating a data source** 1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Data Source**. 2. Click the **Download** icon to resynch data sources from IBM Security Guardium. 3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory**. 4. Click the **Add Data Source** icon to create a data source. 5. Specify all the necessary information. 6. Click **Save**. **Creating and deploying the policy** 1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Policieis**. 2. Click the **Download** icon to resynch classifier policies from IBM Security Guardium. 3. Go to **Business Context Modeler** > **Policy Management Central**. 4. Click the **Add Policy** icon to create a policy. 5. Specify the necessary details. 6. Click **Save**. 7. Deploy the policy in the IBM Security Guardium.

IBM Security Guardium is not displayed in the inventory

Problem	IBM Security Guardium is not listed in **Security Command and Control Center** > **Inventory** > **Data Infrastructure**.
Cause	Guardium appliance is incorrectly configured.
Resolution	Ensure that IBM Security Guardium is configured correctly. 1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration**. 2. Select **IBM Guardium**. 3. Review the configuration details and update as necessary. 4. Click **Test Connection**. 5. Click **Save** after the successful connection to IBM Security Guardium.

Cleansing and analysis problems and workaround

Troubleshoot problems that occur during cleansing and data analysis.

Unavailability of scanned data source in Analysis Workbench for cleansing

Problem	The scanned data source is not found in **Analysis Workbench**.
Cause	Data source is already scanned and the result set is exported to IBM Data Risk Manager Dashboard.
Resolution	An expected system behavior.

Rolling back of levels in Analysis Workbench does not work

Problem	Attempted roll back of levels in **Analysis Workbench** does not work.
Cause	Rollback of levels is not supported in **Analysis Workbench** after the assets are exported.
Resolution	None

Taxonomy mapping and publish problems and workaround

Troubleshoot problems that occur during IBM Data Risk Manager taxonomy mapping and publish.

Default taxonomy attribute values are not mapped

Problem	For the selected asset, taxonomy attributes do not have any values assigned by default.
Cause	Incorrect configuration and mapping of business context data.
Resolution	1. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`) with administrator privileges. 2. Click the application navigation icon ⠿. 3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**. 4. Select the `Database`, `Application`, and `Business Process` CSV files. 5. Click **Load**. 6. Click on Configuration settings icon on the right. 7. Ensure that the **Application** attribute is correctly configured on the `Application` sheet. 8. Click **Save**. 9. Click **Import** to import the context data with necessary changes.

Taxonomy page does not show exported assets

Problem	After cleansing, the asset is not displaying in the **Security Command and Control Center** > **Taxonomy** > **Structured** > **Newly Discovered Assets** page.
Cause	Incorrect configuration and mapping of business context data.

Resolution	1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**. 2. Select the `Database`, `Application`, and `Business Process` CSV files. 3. Click **Load**. 4. Click on Configuration settings icon on the right. 5. Ensure that the **Database Name** and the **IP Address** attributes are correctly configured on the `Database` sheet. 6. Click **Save**. 7. Click **Import** to import the context data again.

Values for the Business Owner and Custodian fields are not populated

Problem	The **Business Owner** and **Custodian** fields are empty for a newly discovered asset.
Cause	Incorrect configuration and mapping of business context data.
Resolution	1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**. 2. Select the `Database`, `Application`, and `Business Process` CSV files. 3. Click **Load**. 4. Click on Configuration settings icon on the right. 5. Ensure that the **Database Name** and the **IP Address** attributes are correctly configured on the `Database` sheet. 6. Click **Save**. 7. Click **Import** to import the context data again.

Information asset is not available in the multiple programs after export

Problem	After the information asset is exported to multiple programs, the asset is not available in those programs.
Cause	Data source is not included in the program scope.
Resolution	Ensure that the data source is entitled to the program scope. 1. Go to **Business Context Modeler**. 2. Select the program to which you want to include data source and click the program name to edit the program. 3. Click the **Scope** icon. 4. Under **Scope**, click the **Data Source** icon. 5. Select the data source for the asset that is not visible, and include it within the program scope. 6. Click **Assign**.

Integration problems and workaround

Use the information in this section to troubleshoot problems that you might encounter during IBM Data Risk Manager installation, uninstallation, or migration process.

Integration problems with Symantec DLP

Troubleshoot problems that occur during IBM Data Risk Manager integration with Symantec DLP.

Unstructured tab not available in Taxonomy

Problem	Unable to see the **Unstructured** option in the **Taxonomy** module.
Cause	• Incident JAR file is not loaded correctly. • Symantec DLP is not configured in the **Integrated Adapter Configuration** module.
Resolution	**Upload the Incident JAR file** 1. Download the incident JAR file at https://support.symantec.com/en_US/article.DOC9265.html. 2. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`). 3. Click the application navigation icon ⁝⁝⁝. 4. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Policies**. 5. Click the download icon ⤓. 6. Select your **Symantec DLP** instance. 7. Click **Choose File** to select and upload the Symantec Incident JAR file. **Configure Symantec DLP** 1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**. 2. Select **Symantec DLP**. 3. Click the **Add Instance** icon to create an instance for Symantec DLP. 4. Specify the necessary details. 5. Click **Save**.

Symantec DLP scan failure

Problem	Failure message when you import the Symantec DLP scans.
Cause	1. Incident JAR file is not loaded correctly. 2. Incorrect URL. 3. Configuration of wrong Report ID.

Resolution	**Uploading the correct Incident JAR file** 1. Download the incident JAR file at https://support.symantec.com/en_US/article.DOC9265.html. 2. Log on to IBM Data Risk Manager Application Suite (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`). 3. Click the application navigation icon ⠿. 4. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Policies**. 5. Click the download icon ⤓. 6. Select your **Symantec DLP** instance. 7. Click **Choose File** to select and upload the Symantec Incident JAR file. **Verifying the URL** 1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**. 2. Select **Symantec DLP**. 3. Check whether the specified URL is correct. **Verifying the Report IDs** 1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Adapter Configuration**. 2. Select **Symantec DLP**. 3. Check whether the specified Report IDs are correct.

Failure when CSV file with incidents is imported

Problem	Failure message is displayed when a CSV file with incidents is imported.
Cause	• Target is not created in IBM Data Risk Manager. • Incorrect target path is specified. • Target is not entitled to a program.

Resolution	**Create a target for Symantec DLP in IBM Data Risk Manager** 1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**. 2. Click **File Storage**. 3. Click the **Add Data Source** icon. 4. Specify necessary details for the target creation. 5. Click **Add**. **Verify the target path** 1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Manage Inventory** > **Data Source**. 2. Click **File Storage**. 3. Select the data source and click the edit icon. 4. Ensure that the path in **Target Path** is correct. 5. Click **Save**. **Target is not entitled to the program** 1. Go to **Business Context Modeler**. 2. Select the program to which the target must be entitled and click the program name to edit program. 3. Click the **Scope** icon. 4. Under **Scope**, click the **Data Source** icon. 5. Select the target data source. 6. Click **Assign**.

Integration problems with IBM Security Guardium

Troubleshoot problems that occur during IBM Data Risk Manager integration with IBM Security Guardium.

VA scope selection options are empty when vulnerability scan is triggered

Problem	Unable to view the scope items when vulnerability scan is triggered.
Cause	Context data is not imported.

Resolution	Import context data and add the assessment. 1. Log on to IBM Data Risk Manager Application Suite (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`). 2. Click the application navigation icon . 3. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Organization**. 4. Click the CSV icon to select the `Database`, `Application` and `Business Process` sheets. 5. Click **Load**. 6. Click the **Configuration Settings** icon. 7. Ensure that the `Database`, `Application` and `Business Process` sheet are configured correctly. 8. Click **Save**. 9. Click **Import** to import the context data with changes applied. 10. Go to **Vulnerability Management**. 11. Click **Create New Assessment**. 12. Click **Scope** to view entities for the updated import of business context data.

On triggering vulnerability scans, the VA tests becomes empty

Problem	Unable to view the list of VA tests when VA scan is started.
Cause	VA tests are not imported from IBM Security Guardium.
Resolution	Import the VA tests from IBM Security Guardium. 1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **VA Tests**. 2. Click the **Download** icon to download VA tests for all the database types from IBM Security Guardium.

IBM Security Guardium appliance list is empty after assessment process is created

Problem	IBM Security Guardium appliance list is empty when the scan process is started.
Cause	IBM Security Guardium appliance is not configured to run VA.
Resolution	1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Integration** > **Integration** > **Adapter Configuration**. 2. Select **IBM Guardium**. 3. Select the instance from the list. 4. Ensure that **Run VA** is selected for the IBM Security Guardium appliances where VA scans are to be triggered.

While remediating the VA scans, the predefined activity list is empty

Problem	Predefined activity list is empty while authoring action items to remediate failed vulnerabilities.
Cause	Solution package is not imported.

Resolution	Ensure that the solution package is imported. 1. Go to **Business Context Modeler** > **Enterprise Integration Wizard** > **Solution Package**. 2. Click **Browse** under **Solution Package** to select the CSV files. 3. Click **Load**. Review the files for correctness. 4. Click **Import** to import the policies and tasks to the IBM Data Risk Manager server. 5. Go to **Vulnerability Management** > **Results View**. 6. Select the failed vulnerabilities based on severity level **Critical** and click **Remediate**. Predefined activities are listed.

Risk value is not displayed for the data sources in the IBM Data Risk Manager dashboard

Problem	Risk value is not displayed for the data sources in the **Infrastructure** widget of IBM Data Risk Manager dashboard even when the data sources contain failed vulnerabilities.
Cause	• Risk frequency is not set. • Infrastructure risk is not configured.
Resolution	**Set the risk frequency** 1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`). 2. Click the application menu icon ⠿. 3. Click **Administration**. 4. On the **Administration** page, click **Server Configuration** > **Deployment Settings**. 5. Set the risk frequency according to the requirements. 6. Click **Schedule**.

DAM alerts are not sent from IBM Security Guardium

Problem	DAM alerts are not sent from IBM Security Guardium.
Cause	• Remote log is not configured on the IBM Security Guardium appliance. • Message template for syslog is not defined correctly in the IBM Security Guardium appliance.

Resolution	**Configuring remote log on the IBM Security Guardium appliance**
	1. Configure Secure Shell (SSH) on the IBM Security Guardium appliance as the user `cli`.
	2. Verify that the appliance is configured to have the IBM Data Risk Manager server as a log destination by specifying the following command.
	`show remotelog`
	3. If the output of the command returns IP address and the syslog port of the IBM Data Risk Manager server, then the configuration is correct. Else, create the remote log entry by using the following command.
	`` store remotelog add non_encrypted `all.all` <ip_address>:<port> tcp ``
	Checking message template
	Ensure that the message template for syslog is defined correctly on the IBM Security Guardium appliance.

DAM alerts are not tagged to assets and data sources

Problem	DAM Alerts are not tagged to the assets and infra node in the dashboard.
Cause	• DAM listener micro service is not running. • DAM listener micro service is logging error message.

Resolution	**Starting the micro service**
	1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
	2. Click the application menu icon ⋮⋮⋮.
	3. Click **Administration**.
	4. On the **Administration** page, click **Diagnostics**.
	5. Check whether the DAM listener micro service is stopped. Run the following command to check the status.
	`service listener status`
	6. If the service is stopped, run the following command to start the service.
	`service listener start`
	Checking the log files
	1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://`*`<IDRM-Server-IP-Address>`*`:8443/albatross/a3suite`).
	2. Click the application menu icon ⋮⋮⋮.
	3. Click **Administration**.
	4. On the **Administration** page, click **Diagnostics**.
	5. Select the **DAM LISTENER** micro service.
	6. Click **Logs**.
	7. Click **Operational**.
	8. Click **Download** under **Download Multiple Logs**.
	9. Review the operational logs.
	10. Contact IBM support if the error messages are logged.

DAM threat not created

Problem	DAM threat is not created.
Cause	• DAM listener micro service is not running. • DAM listener micro service is logging error messages. • Threat occurrence time is incorrect. • The cron job is not running.

Resolution	**Starting the micro service**
	1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
	2. Click the application menu icon ⠿.
	3. Click **Administration**.
	4. On the **Administration** page, click **Diagnostics**.
	5. Check whether the DAM listener micro service is stopped. Run the following command to check the status.
	`service listener status`
	6. If the service is stopped, run the following command to start the service.
	`service listener start`
	Checking the log files
	1. Log on to IBM Data Risk Manager Application Suite with administrator privileges (`https://<IDRM-Server-IP-Address>:8443/albatross/a3suite`).
	2. Click the application menu icon ⠿.
	3. Click **Administration**.
	4. On the **Administration** page, click **Diagnostics**.
	5. Select the **DAM LISTENER** micro service.
	6. Click **Logs**.
	7. Click **Operational**.
	8. Click **Download** under **Download Multiple Logs**.
	9. Review the operational logs.
	10. Contact IBM support if the error messages are logged.
	Editing threat occurrence time
	1. Log on to the IBM Data Risk Manager graphical user interface.
	2. Click the application navigation icon ⠿.
	3. Go to **Business Context Modeler** > **Policy Management Central**.
	4. Click the **Select Policy Type** icon.
	5. Select **Database Activity Monitoring**.
	6. Select the policy for which DAM threat was defined.
	7. In the Policy Rules and Metrics section, click the icon.
	8. Click the **Remediation** icon on selected rule.
	9. To edit the threat configuration information, click the + icon.
	10. Edit the threat occurrence time.
	11. Click the **Save** icon.
	Checking status of cron jobs
	1. Click **Diagnostics** on the **Administration** page.
	2. Select the **DAM LISTENER** micro service.
	3. Click **Logs**.
	4. Click **Download** under **Download Multiple Logs**.
	5. Contact IBM support if the error messages are logged for cron jobs.

Risk associated with DAM threats are not mapped on the IBM Data Risk Manager dashboard

Problem	Risk is not being calculated for DAM threat for the associated data source in the **Infrastructure** widget on the IBM Data Risk Manager dashboard.
Cause	• Risk frequency is not set. • Infrastructure risk is not configured.
Resolution	**Set the risk frequency** 1. Log on to IBM Data Risk Manager Application Suite. 2. Click the application menu icon ⠿. 3. Click **Administration**. 4. Click **Server Configuration** > **Deployment Settings**. 5. Set the risk frequency according to the requirements. 6. Click **Schedule**.

No response message is displayed when running operations in IBM Data Risk Manager

Problem	No response message is displayed when you run any operation in IBM Data Risk Manager.
Cause	
Resolution	The application server might be down. Contact the System Administrator.

High availability configuration problems and workaround

Troubleshoot problems that occur during IBM Data Risk Manager high availability configuration.

Unable to configure IBM Data Risk Manager VM instances for high availability

Problem	Problems when configuring IBM Data Risk Manager high availability.
Cause	Services might have stopped in Primary Node, DB Node, or Application Nodes.

Resolution	**Primary Node**
	1. Log on to the IBM Data Risk Manager virtual machine (VM) instance as a3user over SSH.
	2. Check health status of the following services that are configured with IBM Data Risk Manager.
	From the command line, run the following commands to check status of the load balancing server and Master Database.
	`sudo service httpd status`
	`sudo service postgresql-10 status`
	If the services are stopped, run the following commands to start the services.
	`sudo service httpd start`
	`sudo service postgresql-10 start`
	DB Node
	1. Log on to the IBM Data Risk Manager virtual machine (VM) instance as a3user over SSH.
	2. From the command line, run the following command to check status of the Slave Database.
	`sudo service postgresql-10 status`
	If the database service is stopped, run the following command to start the service.
	`sudo service postgresql-10 start`
	Application Node
	1. Log on to the IBM Data Risk Manager virtual machine (VM) instance as a3user over SSH.
	2. From the command line, run the following command to check status of the application server.
	`sudo service tomcat status`
	If the server is stopped, run the following command to start the server.
	`sudo service tomcat start`
	3. Check health status of the following micro services that are configured with IBM Data Risk Manager.
	From the command line, run the following commands to check status of the services.
	`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`
	If any of the services is stopped, run the respective commands to start the service.

Legal information

Contents

Accessibility features for IBM Data Risk Manager

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in IBM Data Risk Manager:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

Copyright statement

Note: This edition applies to version 2.0.6 of IBM Data Risk Manager (product number 5655-STP) and to all subsequent releases and modifications until otherwise indicated in new editions.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability
These terms and conditions are in addition to any terms of use for the IBM website.

Personal use
You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use
You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights
Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at http://www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Index