IBM Security Identity Governance and Intelligence
Version 5.2.1

Glossary Topics

IBM Security Identity Governance and Intelligence
Version 5.2.1

Glossary Topics

Table of contents

Table list

Glossary

Use the glossary to find terms and definitions that are used by IBM® Security Identity Governance and Intelligence.

The following cross-references are used:

- See refers you from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- See also refers you to a related or contrasting term.

To view glossaries for other IBM products, go to www.ibm.com/software/globalization/terminology.

A

AC See access certifier.

access certifier
The Identity Governance and Intelligence module that certifies users in an organization. The access certifier (AC) module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and segregation of duties (SoD) policies that are enforced by the IBM Security Identity Governance and Intelligence platform.

access governance core
The Identity Governance and Intelligence module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access optimizer
The Identity Governance and Intelligence module that does risk analysis and role mining. Access optimizer (AO) is fully integrated withIdentity Governance and Intelligence role management features to support continuous role development and optimization as business processes evolve.

access requests
The Identity Governance and Intelligence module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk controls
The Identity Governance and Intelligence Access Risk Controls (ARC) module defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP
The Identity Governance and Intelligence Access Risk Controls for SAP (ARCS) module defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

ACCM
See user-account matching.

account
The IT representation of an identity in an IT application where such an identity must operate. An account is the set of user information (UID, email, password, status) that a generic IT system needs to be able to accept or refuse log on by a user.

account attribute
See attribute

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter profile
Defines the type of managed resource.

adoption policy

AG core
See access governance core.

AO See access optimizer.

application
A set of permissions that are related to a certain target (for example, Active Directory).

application role
See IT role.

application server
A server program in a distributed network that provides the execution environment for an application program.

ARC See access risk control.

ARCS See access risk control for SAP.

AR See access requests.

attribute
A characteristic or trait of an entity that describes the entity; for example, the telephone number of an employee is one of the employee attributes.

attribute group (polyarchy)
In the Identity Governance and Intelligence data model, a polyarchy provides different organizational views in hierarchical notation. A generic hierarchy is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

authentication
The first step in the authorization process, based on the credentials that are entered by a user.

authorization
The authorization process defines the level of access, granted to a user, to the resources of a company or organization. In the RBAC model, the authorization profile of a user is based on a set of access rights to the company or organization resources.

authorization profile
It determines what a user can do within the realm and the resources available to the user.

B

BRole See business role.

business activity
See activity.

business process
A group of activities. See also activity.

business role
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

campaign
A series of activities associated with the Identity Governance and Intelligence data model elements.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

cluster
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

connector
A component that provides data connectivity and extraction capabilities for external data sources.

D

dashboard
A graphical user interface that enables users to monitor and manage activities. A dashboard provides a consolidated view of status information that is obtained from various sources.

dashboard items
Special types of reports. They are associated with a query, which produces the data to display.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data point
A calculated value of a metric at a point in time.

data set
A collection of data, usually in the form of rows (records) and columns (fields) and contained in a file or database table.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

E

enterprise connector
The Identity Governance and Intelligence module that aligns the central IDEAS database with the peripheral target systems and vice versa.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

event A short set of information that provides the interaction between Identity Governance and Intelligence AG core and an external target system. Each time data change must be spread to different system components; the changes are copied into the appropriate packages (events) and sent to listening systems if necessary.

event marker
Represents the target system as the sender or recipient of connected events to or from Identity Governance and Intelligence.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). An external role is received directly from a connected target through the Bulk load tool.

F

farness
A numeric index that provides an estimate of the virtual distance between OUs having the same entitlement/candidate role. It can measure the distance between OUs in which different registered users are assigned the same entitlement/candidate role.

H

home directory
The directory associated with the product.

I

IAG See Identity and Access Governance.

IAG activity
A part of an Identity and Access Governance Process.

IAG actor/operator
A user that has one or more IAG roles.

IAG administrator
An administrator that can assign IAG roles.

IAG process
A set of activities that support an authorization process.

IBM Security Identity Governance and Intelligence
IBM Security Identity Governance and Intelligence delivers one platform for organizations to analyze, define, and control user access and access risks. It uses business-centric rules, activities and processes, empowering line-of-business managers, auditors, and risk managers to govern access and evaluate regulatory compliance across enterprise applications and services.

Identity and Access Governance
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

Identity Brokerage

The gateway to directly integrate Identity Governance and Intelligence with targets and hubs by using IBM Security Identity Manager Adapters. These IBM Security Identity Manager Adapters are called Identity Brokerage Adapters in Identity Governance and Intelligence.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

job In the task planner module, a single logical unit of code that defines the execution of a function (possibly containing several steps).

M

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed.

minability
Indicator of the efficiency of aggregating assignments into roles. It provides a measure of how to easily build and define a role.

N

node A logical group of managed servers.

O

object class
A categorization or grouping of objects that share similar behaviors and circumstances.

organization unit
An organization can be broken down into organization units (OUs), each of which can in turn comprise other small units, all of which together form a hierarchical tree structure. It is one of the main elements of the Identity Governance and Intelligence data model. It implements the main hierarchy of Identity Governance and Intelligence. Moreover, Identity Governance and Intelligence supports other hierarchies, named "polyarchies" (see also attribute group) that can provide different organizational views in hierarchical notation, grouping users by attribute values.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OU See organization unit.

P

PD See process designer.

permission
The elementary authorization object that is defined as an operation on protected objects (such as reading and writing local files, creating connections). It is a specific type of entitlement (see also entitlement).

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

polyarchy
See attribute group.

primary node
A cluster node that currently has the principle copy of a cluster resource. All replications of a resilient resource originate from the primary copy of the resource.

private key
An algorithmic pattern that is used to encrypt messages that only the corresponding public key can decrypt. The private key is also used to

decrypt messages that were encrypted by the corresponding public key. The private key is kept on the user system and is protected by a password.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer
Process designer (PD) is the Identity Governance and Intelligence module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

R

RBAC See role-based access control.

RD Report designer (RD) is the Identity Governance and Intelligence module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

realm A model that describes an organization in terms of a set of "objects" (users, organization units, entitlements, applications, resources) and the relationships that exist between them (IBM Security Identity Governance Data Model). Users in an organization belong to the same realm.

reconciliation
The process of synchronizing a target system with the server. It removes old and obsolete objects from the server to ensure consistency between the repositories.

resource
Any kind of company resource that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, network folders, documents, and any other logical or physical object that is useful for access governance.

right An extra attribute that is related to a permission. A right is defined by two attributes, key and value.

risk A concept that is useful for modeling a wide range of possible threats or potential damages that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into the Identity Governance and Intelligence data model. The aim is to detect every risk by the business rules violation.

role Identifies the set of permissions and resources to which the person has access. A user can be assigned one or more roles. Any role can be associated with any set of tasks, dashboards, reports, campaigns, and other resources.

role-based access control
A method for restricting system access to authorized users. The NIST/ANSI/INCITS RBAC standard (2004) recognizes three levels of RBAC: 1) core RBAC, 2) hierarchical RBAC, which adds support for inheritance between roles, and 3) constrained RBAC, which adds segregation of duties.

role mining
The process of analyzing the set of permissions and resources to which the person has access.

rule Is a logic statement that is used to help tailor Identity Governance and Intelligence to the business processes of your organization. Rules are defined to run specific actions upon the detection of specific events.

S

scope In the Identity Governance and Intelligence model, use scope to define different types of operational limitations for the IAG actors (administrator and users) from the Identity Governance and Intelligence data model entities (OUs, applications, entitlements, activities).

security questions
A set of questions that the user must answer for identity verification and authentication.

segregation of duties
Identity Governance and Intelligence reveals segregation of duties conflicts that arise after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements. A conflict of interests.

self care
An Identity Governance and Intelligence application available in the Service Center. Within the Self Care application, employees can change their account passwords, view their password change requests, and update their security questions.

self-signed certificate
In cryptography, a public key certificate that is signed with its own private key rather than by a certificate authority.

SoD See segregation of duties.

spread
A numeric index that provides an estimate of the "homogeneous diffusion" of a role in the hierarchical structure of an organization.

system administrator
The person who controls and manages a computer system.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java Archive (JAR) file that contains the profile.

target type
Also called target profile, is a category of related targets that share schemas. It defines the schema attributes that are common across a set of similar managed resources. It is defined in the target definition file of an adapter.

target system
Repositories for user account information.

task A set of jobs (TP module), linked together to form a complex function to be run.

task planner
The Identity Governance and Intelligence module that manages “asynchronous” Identity Governance and Intelligence processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

trace A record of the processing of a computer program or transaction. The information that is collected from a trace can be used to assess problems and performance.

trace level
A level associated with each trace point. The level of a trace point depends on where the trace point is and on what sort of detail it can provide on a trace call. Most trace points are trace level 1 or 2.

TP See task planner.

U

UME See user multiple entries.

user A user is a set of information, "digital identity," that identifies an individual or a virtual identity (such as service users). Identity Governance and Intelligence supports the concept of primary and secondary users (see also UME).

user multiple entries
Identity Governance and Intelligence supports the concept of primary and secondary users. Although they are separate users for many organizational reasons, the system tightly connects the primary master user with secondary users and UME by automatically maintaining synchronization of any user information changes. Different roles and permissions can be granted to UME; Identity Governance and Intelligence automatically complements authorizations for sensible analysis such as SoD and risks.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

V

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

W

workflow
The structured sequence of activities and tasks performed in accordance with the organization's business processes.

Index

G

Printed in USA