SailPoint - IdentityIQ Essential

Table of Contents

IdentityIQ Essentials

We create Identity Cubes in IdentityIQ when we aggregate accounts from an **authoritative application**, also known as **system of record**, and this can be a HR application or Active Directory.

When an aggregation reads in data from an external source, a **refresh** calculates information on the Identity Cubes and can detect violation of policies and calculates risk scores.

IdentityIQ Extended Attributes

- Several objects can be extended:
    - Applications
    - Roles (bundle)
    - Certification Items
    - Identities
    - Accounts (link)
    - Entitlements (managed attributes)
- Marking an attribute as *searchable*, or not, defines how it will be stored in the database
- An Identity Attribute *not* marked searchable through GUI, will be stored in a CLOB (Character Large Object) data type, and it's an efficient way to store large amounts of data
- Multiple extended attributes can be stored in a **single** CLOB attribute
- An attribute marked as *searchable* is stored in its own column in the database
- An attribute stored in a CLOB can still be access, but **performance will suffer**

There are 3 types of searchable attributes:

1. Standard Attributes

   Predefined by IdentityIQ

2. Named Extended Attributes

   Defined by user

3. Placeholder Extended Attributes

   An attribute marked as searchable but without a name column defined. In that case, iiq will use a placeholder column for it (such as *extended1*)

1. Configure IdentityIQ

1. Confirm the installation of IdentityIQ
   - Using a linux terminal in the machine where IdentityIQ is installed, navigate to `~/tomcat/webapps/identityiq/WEB-INF/bin` and run the following command:

     ```
     ./iiq console -j
     ```

     > The `-j` option enables using the arrow keys to page through commands entered during the session.

   - Run the following command: `about`
   - The **Version** line lists the iiq version. patch version and the build
   - Enter `quit` to exit the console
2. Explore IdentityIQ
   - Navigate to IdentityIQ url: *http://localhost:8080/identityiq/*
   - Log in to iiq as the iiq Administrator: **spadmin / admin**

2. Create Database

1. Generate Database Schema (DDL)

   Create IdentityIQ database:

   .../WEB-INF/bin/iiq schema

2. Extend Database

   Create delta DDL

   .../WEB-INF/bin/iiq extendedSchema

3. Configure IdentityIQ Properties

   Identify database to iiq

   .../WEB-INF/classes/iiq.properties

4. Initialize IdentityIQ Default Objects
    - Initialize iiq

```
.../WEB-INF/bin/iiq console
import init.xml
```

    - Initialize iiq Lifecycle Manager

```
.../WEB-INF/bin/iiq console
import init-lcm.xml
```

3. Define Application

- Representation of the imported source in SailPoint
- *Applications/Application Definition/Add New Application*

4. Aggregation Task

- *Setup/Tasks/New Task/Account Aggregation*
- **Generation of the Identity Cubes** from the defined applications
- In *Identity/Identity Warehouse* you can find the generated identitites
- In *Identity/Identity Warehouse/Application Accounts* there are the Application Accounts Data
- In *Identity/Identity Warehouse/Attributes*, the Attributes sections is still blank because **there is no mapping between the identity attributes and the application yet**

5. Define and Map Identity Attributes

- In *Gear/Global Settings/Identity Mappings* you can populate both Standard and Extended Identity Attributes from the Application Accounts

6. Refresh Identity Cubes

- In *Setup/Tasks/Refresh identity Cube* it is possible to refresh the Identity Cubes in order to apply the mapped attributes at point 3

Capabilities

Identities > *Identity Warehouse* > *User Rights*

- Define what additional rights a user has **within IdentityIQ**
- Control which menu options are available

Default User Rights includes:

- Home Page
- Quicklinks

- My Work

Scoping

- The act of subdividing data into logical groups and granting access based on those subdivision
- Scopes control the objects a user can see and act upon

Workgroups (set of identity)

- Group of IdentityIQ users used for:
    - Assigning access to IdentityIQ (capabilities, scopes)
    - Sharing IdentityIQ responsabilities:
        - Team-assigned work items
        - Object ownership (best practice)

Populations (query)

Intelligence > Advanced Analytics

- A population is a **saved query** that defines a set of identities that share a common set of attribute (can be created from **multiple search criteria**)
- Used as a filter on the set of identities included in a task, certification or report
- Manually created

Groups (query)

Setup > Groups > Create New Group

- Collection of IdentityIQ users **based off a single identity attribute** (that must be checked as *Group Factory* in the *Identity Mapping*) and used to define target of operation (e.g. task filter, report filter)
- Used to filter identities included in a task, certification or report
- Groups can be created by marking an identity attribute as *group factory*
- Automatically created by running the *Refresh Group* task, instead of manually creating populations
- A Group is stored as a **query**

Examples:

1. *Group Factory = Location*
2. Running *Refresh Groups* Task
3. Sub-Groups of Location: Austin, London, Sydney ...
4. Members in the Sydney sub-group: Alex, David, Julia etc

Create Populations

1. Navigate to *Intelligence/Advanced Analytics*
2. Make sure *Search Type* is *Identity* and click *Clear Search*
3. Select *Is Inactive: False* and *Type: Employee* and click *Run Search*
4. From the *Result Options* drop down menu, select *Save Identities as Population*
5. Set *Name: Active Employees* and *Description: Active employee identities*

6. Update the population's visibility to public from *Setup/Groups/Populations* click the Population's name, uncheck *private* and save

Create Groups

1. Navigate to *Setup/Groups/Groups tab* and click *Create New Group*
2. Generate Groups using the newly created group configuration
    - Navigate to *Setup/Tasks* and search for *Refresh Groups*
    - *Save and Execute*
    - Check the groups

Create Workgroups

1. Navigate to *Setup/Groups/Workgroups* and click *Create Workgroup*

Non-Authoritative Applications

Authoritative Applications

- Sources that provide a definitive list of people within the company

Non-Authoritative Applications

- Sources that provide additional accounts and entitlements for people within the company
    - Finance systems
    - Document sharing systems
    - etc

Account Schemas

- Account schemas define which account attributes to read from an application when aggregating accounts with IdentityIQ

Entitlement Catalog / Identity Cube

In *Applications* > *Application Definition* > *Configuration* > *Schema* > *Attributes* it is possibile to add these properties in the Properties colums:

- Managed
    - For every value of the attribute, we'll add an entry to the entitlement catalog (this is why internally an *entitlement* is called *managed attribute*)
- Entitlement
    - Each value of the attribute will be marked as an entitlement on the user's cube
- Multi-Valued
    - The user can have more than one value for the attribute

Group Schema

> **These are Account Group, so they are related to the account from the target system (such as LDAP or AD groups), NOT groups created from Setup > Groups > Create New Group**

- Groups which grant/identitfy user access on other systems (applications) and loaded into IdentityIQ through (account group) aggregation
- Optional, but common with non-authoritative applications
- The group schema is how we define the attributes that define account groups on the system we are reading from
- Groups are managed in Entitlement Catalog
- The entitlement catalog shows whether the entry is based on a group definition by marking the type as "group" (otherwise marked as "entitlement")

Account Correlation

- Matches an account to an authoritative Identity Cube
    - If no correlation, non-authoritative cube is created
- Options for configuring correlations:
    - Rapid Setup correlation
    - Correlation Wizard
    - Correlation rule

IdentityIQ Connectors

Connector

- Software component to connect to business resource and read/write data
- Provides normalized resource object

Application

- Any data source with which IdentityIQ communicates to manage governance and compliance for your enterprise (HR System, AD, etc)
- Includes configuration details

Logging

- Standard Out print statements (Not recommended for production because sensitive info can be leaked and the *catalina.out* may get filled quickly)
- Java application logging (log4j)
- Email redirection
- Audit configuration
- Syslog logging configuration

The logging levels in the order from the least critical to the most critical is the following:

1. trace
2. debug
3. info
4. warn
5. error
6. fatal (rarely used)

System.out vs Log4j

```
System.out.println("I'm logging this message all the time.");
log.debug("I'm logging this message when debug is turned on.");
```

Advantages of using Log4j:

- Reduced Size of `catalina.out`:
  - Logs are separated from catalina.out, preventing it from becoming bloated
- Log Rotation and Size Limits:
  - Automatic log rotation based on size or time
  - Ability to set size limits on log files
- Archiving and Compression:
  - Automatic archiving of old logs
  - Compression of logs to save disk space
- Selective Logging to Control File Growth:
  - Control logging output by setting log levels (e.g., DEBUG, ERROR)
  - Granular logging for specific components or time periods
- Easier Maintenance:
  - Smaller, organized log files make maintenance and review easier
  - Reduced overall disk space usage for logs

File settings path: `<install dir>/WEB-INF/classes/log4j2.properties`.

The `rootLogger` set the default log level for the whole application, but you can also configure logging levels for individual Java classes.

```
// Log4j Example

log.error("This is an error message");
log.warn("This is a warn message");
log.info("This is an info message");
log.debug("This is a debug message");
log.trace("This is a trace message");
```

In the example above, if the logging level in the `log4j2.properties` file is set to `warn` like the following

`rootLogger.level=warn`

the more severe logging levels are printed too, so `This is a warn message` and `This is an error message` get printed.

> Because of the sheer volum of messages Trace produces it's often better to start with Debug when you are troubleshooting a process

IdentityIQ Console

- Command-line interface
- Authentication required (only users with the System Administrator capability ca access the console)
- Connects directly to database
  - Can be used to troubleshoot connectivity problems
- Some commands are only available via console
  - SQL query interface
  - Export

Data Export Best Practice

- Remove information unique to IdentityIQ instance (`id`, `created`, `modified`)
  - Use export and checkout `clean` option
  - Import `noid` option

IdentityIQ Policies

> IdentityIQ policies define user access conditions that are *unwanted* by the organizations.

- Detect users who are currently in violation of policies
- Prevent users from violating policies

Policy Examples

- Mutually exclusive access
- Incorrect responsibilities
- More than one account

IdentityIQ Certifications

A Certification or Access Review is nothing more than the process of automating the periodic review and approval of certain things such as:

- Identity Access
- Role Membership
- Account Group Membership
- Role Composition
- Account Group Permissions

Purpose

- Keep user access compliant
  - Legal requirements
  - Industry standars or regulations
  - Business rules
- Provide oversight and visibility

Responsabilities

- Implementers and system administators
    - Responsible for knowing how these features work
    - Possibly responsible for providing rules
        - Unlikely to be responsible for ongoing configuration and monitoring
- Often companies have dedicated compliance teams/business administrators

Access Certifications

- The process of automating the periodic review and approval of:
    - Identity Access
    - Role Membership
    - Account Group Membership
    - Role Composition
    - Account Group Permissions

Certifications/Access Reviews

Certifications

- Define the certification campaign
    - What is reviews
    - When
    - By whom
- A certification is composed of one or more Access Reviews

Access Reviews

- Gather users' access data at time of generation
- Provide that collection of data to be certified
- Routed to the reviewer to take action

Access Review Details

- The detail of an Access Review
- Present the entities to be certified

Trigger Certifications

- Mulitple options for triggering certifications
    - Manual creation
    - Scheduled, recurring
    - Data changed, triggering Certification Event

IdentityIQ Roles

- An object that encapsulates sets of access

Business Role

- Roles associated directly to the identities based on their functions in the business

IT Role

- Each Business Role can be connected to one or more IT roles which logically group related entitlements together

Birthright Roles vs Business Roles

Birthright Roles

- Baseline access, assigned to new personnel
- Only assigned during joiner lifecycle events
- Not requestable
- Single tier

Business Roles

- Access for teams, departments, projects, etc.
- Assigned by Identity Refresh task, "Refresh assigned, detected roles ... "
- Requestable
- Two-tier: required and permitted relationship with IT roles

Provisioning

> Provisioning is the process for managing changes to user and access data, which can include adding, modifying, or removing access.

Provisioning Policies

- Provide values to **create**, **update**, and **delete** accounts on connected applications
  - Values can be provided manually by user
  - Values can be provided by IdentityIQ (auto-calculated or static)

Provisioning Dependencies

- Your company may have dependency requirements where a user's access to an application is dependent on access from another application.
- IdentityIQ allows this through the application dependency configuration found in the application definition (*Configuration* > *Provisioning Policies*).
- You can specify that a user must have an account on another system before we create their account for this system.

Monitor Provisioning

WorkflowCase Object

- Created when action in IdentityIQ triggers a workflow

- Contains details for a running workflow process
- Exists only until workflow completes

WorkItem

- Created by a workflow (or IdentityIQ) to obtain input from a person
- Exists until the input is acquired
- Examples
    - Approvals
    - Policy violations
    - Request for manual provisioning
    - Access review delegations
    - Request for data

Lifecycle Events

- Activities that happen in the normal course of a person's employment
    - Joining the company (joiners)
    - Changing departments/managers (movers)
    - Leaving the company (leavers)

Lifecycle event is a two step process:

1. Starts with an aggregation
2. Ends with a Refresh Task

> To be able to view the lifecycle event details under Track My Requests, you must use a workflow that creates and updates the request record

Quicklink

Quicklink Populations

- Flexible method to control who has access to a Quicklink
- Provide for answering the three questions:
    - Who can request?
    - Which identities can be targeted?
    - What can be requested?

Automated Provisioning

Native Change

- A data change that is discovered at the application account level, during an aggregation process
    - Undesired, unexpected
    - Not following normal process

Other Provisioning Requests

Identity Batch Request

- Batch request management
    - Process mass identity changes via a file upload
- Operations Supported
    - Create/Modify Identity
    - Create/Delete Account
    - Enable/Disable Account
    - Unlock Account
    - Add/Remove Role
    - Add/Remove Entitlement
    - Change Password