SailPoint - IdentityIQ

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 potin 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)

- Set of identities treated as a single identity
- Workgroups are 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** performed in the *Advanced Analytics* that defines a set of identities that share a common set of attributes
- Used as a filter on the set of identities included in a task, certification or report
- Manually created
- Can be created from **multiple search criteria**

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**

Example:

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*

Account Schemas

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

Account Group

- Groups which grant/identify user access on other systems (applications) and loaded into IdentityIQ through (account group) aggregation

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)
- Java application logging (log4j)
- Email redirection
- Audit configuration
- Syslog logging configuration

Print 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.");

Log4j

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

```
// Log4j Example

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